



Universidad
Carlos III de Madrid

DEPARTAMENTO DE INGENIERÍA TELEMÁTICA

TRABAJO FIN DE GRADO

GRADO EN SISTEMAS DE COMUNICACIONES

**ANÁLISIS DEL POTENCIAL DE UNA
INFRAESTRUCTURA CIBER-FÍSICA PARA
TELEGESTIÓN DE CONTADORES INTELIGENTES
BASADA EN SOFTWARE COMERCIAL**

AUTOR: JAVIER OLMEDA DELGADO

TUTOR: DR. JOSÉ IGNACIO MORENO NOVELLA

DIRECTOR: DR. GREGORIO IGNACIO LÓPEZ LÓPEZ

LEGANÉS, FEBRERO DE 2017

Agradecimientos

En primer lugar, me gustaría agradecer tanto a Gregorio López, director de este Trabajo de Fin de Grado, como a José Ignacio Moreno, tutor del mismo, la oportunidad de realizar este proyecto dentro del grupo de investigación del Departamento de Ingeniería Telemática. Agradecer también el trato recibido del grupo de investigación del Profesor José Ignacio Moreno, formado por Gregorio López, junto con Miguel Seijo y Mario Sanz, ya que desde el primer día me hicieron sentir a gusto en su ambiente de trabajo, prestándome además ayuda en tantas dudas como me iban surgiendo, sobre todo Gregorio, cuya ayuda y supervisión han sido fundamentales para la realización de este proyecto. También me gustaría dar las gracias a los miembros del Proyecto OSIRIS que han colaborado de alguna u otra manera, especialmente a Alberto Carracedo (STM Telecontrol) por su inestimable ayuda y su amabilidad.

A mis amigos, los de toda la vida y también los de la universidad, por haber compartido conmigo infinidad de momentos desde el primer día que pisé el campus de Leganés. Ese día, comencé la etapa de mi vida que hoy llega a su fin y que, más allá de la titulación adquirida, me deja en herencia la amistad de las personas que la han compartido conmigo y el recuerdo de los momentos aquí vividos.

En este sentido, mención especial a Blanca, mi novia, a quien he podido conocer en la universidad. Con ella he compartido, y lo seguiré haciendo, grandes momentos durante estos casi tres años en los que se ha convertido en una parte fundamental de mi vida y ha contribuido en gran medida a hacer de mí la persona que soy hoy en día.

Por último, agradecer también de manera especial a mi familia por haber estado ahí durante todos estos años, por la educación que me han dado y los valores que me han inculcado, por haber sido siempre comprensivos conmigo, aunque en ocasiones no mereciera esa comprensión. Agradecerle haberme dado todas las posibilidades en la vida que han estado en su mano y haberme permitido crecer y desarrollarme como persona en el mejor entorno posible.

Resumen

En la actualidad, las Tecnologías de la Información y la Comunicación (TIC) están presentes en la mayoría de los sectores, siendo su uso fundamental para mejorar la productividad y eficiencia de cada uno de ellos. El sector energético no es una excepción y, por tanto, también está incluyendo de manera progresiva estas tecnologías a través de las denominadas redes inteligentes o *Smart Grids*. El presente TFG se centra en las infraestructuras de medición avanzadas (AMI o *Advanced Metering Infrastructures*), que permiten la comunicación bidireccional con los medidores (de consumo y/o generación) inteligentes, con todas las ventajas que ello conlleva tanto para la gestión de la red de distribución eléctrica como para los clientes.

De entre las tecnologías que se utilizan en la “última milla” (comunicación entre medidores inteligentes y concentradores de datos) de las mencionadas AMI destaca PLC (*Power Line Communications*), una tecnología muy atractiva para las distribuidoras eléctricas ya que permite utilizar el cableado eléctrico tradicional para fines comunicativos. Sin embargo, la red eléctrica no fue diseñada originalmente para la transmisión de datos, por lo que es un medio bastante hostil. A pesar de esto, las ventajas que ofrece a las distribuidoras y el buen rendimiento de los diferentes estándares PLC de banda estrecha (NB-PLC) hacen de ella una tecnología idónea para su utilización en este ámbito.

PRIME es un estándar de comunicaciones PLC de banda estrecha utilizado en dicha “última milla”. Se trata de un estándar con una amplia utilización en España y con una gran proyección internacional, promovido y desarrollado por la *PRIME Alliance*, liderada por Iberdrola y Gas Natural Fenosa.

Debido al desarrollo de las *Smart Grids*, la nueva definición de los sistemas de medición inteligentes ya no sólo se refiere a los contadores, sino también a los sistemas de telegestión, fundamentales para poder aprovechar todo el potencial que se deriva del inmenso volumen de datos disponible y de poder controlar cualquier dispositivo de la infraestructura de medición de manera remota. Una de las plataformas de telegestión existentes en el mercado es IRIS, desarrollada por STM Telecontrol, que ofrece numerosas posibilidades de telegestión y telemedida para concentradores y contadores PRIME.

La aparición de estas nuevas tecnologías, protocolos y plataformas tecnológicas hace que el sector eléctrico demande profesionales cualificados que sean capaces de aprovechar todo su potencial y de sacar el máximo rendimiento de ellas. El principal objetivo de este TFG es elaborar un manual de prácticas junto con su solucionario que permita obtener experiencia real sobre cómo funcionan las tecnologías y soluciones mencionadas anteriormente, con vistas a que pueda aprovecharse en alguna asignatura relacionada en el futuro. Para ello, se dispone de una infraestructura ciber-física, formada por dispositivos físicos y virtuales, totalmente telegestionable mediante IRIS.

Este TFG se ha desarrollado en el Departamento de Ingeniería Telemática de la Universidad Carlos III de Madrid, dentro del marco del proyecto OSIRIS (Optimización de la Supervisión Inteligente de la Red de Distribución), financiado por el Ministerio de Economía y Competitividad y liderado por Unión Fenosa Distribución. (tercera distribuidora eléctrica de España en términos de número de contadores).

Palabras clave

Comunicaciones PLC de banda estrecha (NB-PLC); concentrador de datos; contador inteligente (*Smart Meter*); DLMS/COSEM; infraestructura ciber-física; Infraestructuras de Medición Avanzada (AMI); IRIS; plataforma de telegestión; PRIME; *Smart Grids*; STG-DC; ZIV PRIME Manager.

Abstract

Nowadays, Information and Communication Technologies are present in almost every sector, being fundamental to improve the productivity and efficiency of each one of them. The energy sector is no exception and therefore is also progressively including these technologies through so-called Smart Grids. This TFG focuses on Advanced Metering infrastructures (AMI), which allow bidirectional communication with smart meters (consumption and/or generation), with all the advantages that it implies both for network management and for the clients.

Between all of the technologies used in the “last mile” (communication between smart meters and data concentrators) of the mentioned AMI, it outstands PLC (Power Line Communications), a very attractive technology for electrical distributors since it allows the use of traditional electric wiring for communicative purposes. However, the power grid was not originally designed for data transmission, so it is a rather hostile environment. Despite this, the advantages offered to the distributors and the good performance of the different narrowband PLC (NB-PLC) standards makes it a suitable technology for use in this field.

PRIME is a narrowband PLC communications standard used in the last mile. In Spain, it is a wide used standard and with a great international projection, promoted and developed by the PRIME Alliance, led by Iberdrola and Gas Natural Fenosa.

Due to Smart Grids development, the new definition of smart metering systems no longer only refers to meters, but also to remote management systems, which are essential to take advantage of the potential derived from the huge volume of data available and being able to control any device of the metering infrastructure remotely. One of the existing remote management platforms on the market is IRIS, developed by STM Telecontrol, which offers numerous remote management and metering options for PRIME Smart Meters and concentrators.

The emergence of this new technologies, protocols and technological platforms makes it possible that the electrical sector demands highly skilled professionals who are able to leverage all of their potential and to get the maximum performance of them. The main goal of this TFG is to elaborate a lab manual along with its corresponding set of solutions which allows obtaining real experience about how technologies and solutions mentioned above actually work, with views that this manual can be exploited in a future related subject. For this, it is available a cyber-physical infrastructure consisting of both physical and virtual devices fully remotely manageable with IRIS.

This TFG has been developed in the Department of Telematics Engineering of Carlos III University, within the scope of OSIRIS research project, financed by the Ministry of Economy and Competitiveness and led by Unión Fenosa Distribución (third electrical distributor of Spain in terms of number of meters).

Keywords

Advanced Metering Infrastructures (AMI); cyber-physical infrastructure; data concentrator; DLMS/COSEM; IRIS; narrowband PLC (NB-PLC) communications; PRIME; remote management platform; Smart Grids; Smart Meter; STG-DC; ZIV PRIME Manager.

Índice general

Introduction.....	17
1.1 Motivation	18
1.2 Goals.....	21
1.3 Memory structure	22
Estado del arte.....	24
2.1 Arquitectura de comunicaciones para AMI.....	25
2.2 Visión global de las tecnologías PLC de Banda Estrecha	26
2.3 PRIME	29
2.3.1 General.....	29
2.3.2 Capa física	29
2.3.3 Capa MAC	29
2.3.4 Capa de Control de Enlace Lógico (LLC)	50
2.3.5 Capa de aplicación.....	51
2.4 DLMS/COSEM	52
2.4.1 General.....	52
2.4.2 Modelo de comunicación.....	52
2.4.3 Dispositivos físicos y lógicos	53
2.4.4 Funcionamiento orientado a conexión.....	56
2.4.5 Asociaciones de aplicaciones (AAs).....	56
2.4.6 Sistema de Identificación de Objetos (OBIS).....	58
2.4.7 Perfiles de comunicación	59
2.5 STG-DC	61
2.6 Meter Data Management Systems (MDMS).....	62
2.6.1 General.....	62
2.6.2 Plataforma de Telegestión IRIS	63
2.7 Infraestructura ciber-física	65
2.8 Herramientas utilizadas	67
2.8.1 ZIV PRIME Manager	67
2.8.2 Interfaz Web del Concentrador ZIV	67
2.8.3 XML Translator	67
2.8.4 Obis Helper.....	67
2.9 Marco regulatorio	68
2.9.1 Marco regulatorio europeo.....	68
2.9.2 Marco regulatorio español	69
Diseño de la solución.....	70
3.1 Requisitos y restricciones	71
3.2 Manual de practicas	72
3.2.2 Escenario de prueba.....	72
3.2.3 Pruebas.....	73
Resultados y evaluación	78
4.1 Solucionario del manual de prácticas	79
4.1.1 Bloque 1: Protocolo PRIME y ZIV PRIME Manager	79
4.1.2 Bloque 2: PRIME/DLMS/COSEM e Interfaz Web del Concentrador ZIV ..	87

4.1.3 Bloque 3: Comunicaciones extremo a extremo (PRIME/DLMS/COSEM + STG) y Plataforma de Telegestión IRIS	102
Impacto socio-económico	114
5.1 Impacto	115
5.2 Planificación	116
5.3 Presupuesto	117
Conclusions and future works	119
6.1 Conclusions.....	120
6.2 Future Works	122
ANNEX I.....	127
Extended Abstract.....	127
1. Motivation	127
2. Goals.....	130
3. Memory structure	130
4. Conclusions	132
5. Future Works	133
ANEXO II.....	135
Informes y órdenes STG-DC.....	135
ANEXO III	138
Manual de usuario de IRIS	138
1. Introducción.....	138
2. Concentradores	139
3. Colecciones.....	156
4. Firmware.....	158
5. Sistema.....	159
ANEXO IV	162
Manual de usuario de ZIV PRIME Manager.....	162
ANEXO V	167
Manual de usuario de la Interfaz Web del Concentrador ZIV.....	167

Índice de figuras

Figura 1 – Arquitectura de comunicaciones típica para Sistemas de Medición Avanzada	25
Figura 2 – Despliegue de tecnologías NB-PLC en Europa [12].....	26
Figura 3 – Estados funcionales de un nodo de servicio [8]	30
Figura 4 – Estructura de direccionamiento [8]	31
Figura 5 – Asignación de direcciones: fase 1 [8]	31
Figura 6 – Asignación de direcciones: fase 2 [8]	32
Figura 7 – Asignación de direcciones: fase 3 [8]	32
Figura 8 – Estructura de una trama MAC [8]	33
Figura 9 – Ejemplo de tablas de switching [8]	35
Figura 10 – Algoritmo de encriptación AES [8]	36
Figura 11 – Estructura de una GPDU [8]	36
Figura 12 – Campos de la cabecera de una GPDU [8].....	37
Figura 13 – Estructura de un paquete [8]	37
Figura 14 – Campos de la cabecera de un paquete [8]	37
Figura 15 – Campos de la cabecera de una PNPDU [8].....	38
Figura 16 – Campos de una BPDU [8].....	38
Figura 17 – Proceso de registro aceptado [8]	43
Figura 18 – Proceso de registro rechazado [8]	44
Figura 19 – Proceso de cancelación de registro iniciado por un nodo terminal [8]	44
Figura 20 – Proceso de cancelación de registro iniciado por el nodo base [8].....	44
Figura 21 – Proceso de promoción iniciado por un nodo de servicio [8].....	45
Figura 22 – Proceso de promoción rechazado por el nodo base [8].....	45
Figura 23 – Proceso de promoción iniciado por el nodo base [8]	46
Figura 24 – Proceso de promoción rechazado por un nodo de servicio [8]	46
Figura 25 – Proceso de degradación iniciado por un nodo de servicio [8]	46
Figura 26 – Proceso de degradación iniciado por el nodo base [8].....	47
Figura 27 – Establecimiento de conexión iniciado por un nodo de servicio [8]	48
Figura 28 – Conexión rechazada por el nodo base [8]	48
Figura 29 – Establecimiento de conexión iniciado por el nodo base [8].....	48
Figura 30 – Desconexión iniciada por un nodo de servicio [8].....	49
Figura 31 – Desconexión iniciada por el nodo base [8]	49
Figura 32 – Relación y protocolos cliente/servidor [17]	53
Figura 33 – Modelo de servidor COSEM [19]	54
Figura 34 – Sesión de comunicación completa en el entorno orientado a conexión [20]	56
Figura 35 – Secuencia para el servicio COSEM-OPEN [21].....	57
Figura 36 - Estructura del código OBIS [19]	58
Figura 37 – Perfil de comunicación DLMS/COSEM genérico [20]	60
Figura 38 – Esquema de la infraestructura física	65
Figura 39 – Esquema de la infraestructura ciber-física	66

Figura 40 – Escenario de prueba (explicado en detalle en el Apartado 2.7)	72
Figura 41 – Secuencia de BPDUs	79
Figura 42 – Secuencia PRIME de registro	80
Figura 43 - Secuencia PRIME de conexión.....	80
Figura 44 – Intercambio de mensajes PRIME para el proceso de keep-alive	81
Figura 45 – Intercambio de mensajes PRIME para el proceso de keep-alive	81
Figura 46 – Mensaje PRIME de desregistro.....	82
Figura 47 – Mensaje PRIME de solicitud de promoción	82
Figura 48 – Secuencia PRIME de respuesta y reconocimiento de promoción.....	82
Figura 49 – Mensajes PRIME para notificar cambios en las balizas	83
Figura 50 – Posibles frecuencias de transmisión de balizas.....	83
Figura 51 – Valores de los campos de las BPDUs	84
Figura 52 – Mensaje PRIME de solicitud de degradación	84
Figura 53 – Rango de frecuencias PRIME	85
Figura 54 – Modulaciones posibles en PRIME	86
Figura 55 – Constelación PRIME utilizada.....	86
Figura 56 – Secuencia de mensajes PRIME de tipo Data	88
Figura 57 – Estructura de una MAC PDU genérica	88
Figura 58 – Estructura del payload de una GPDU	88
Figura 59 – Identificación en las tramas PRIME del final de un mensaje DLMS/COSEM y comienzo del siguiente	89
Figura 60 – Identificación de las secuencias iniciales de los mensajes DLMS/COSEM AssociationRequest y AssociationResponse	90
Figura 61 – Decodificación en XML de un mensaje DLMS/COSEM AssociationRequest	90
Figura 62 – Decodificación en XML de un mensaje DLMS/COSEM AssociationResponse.....	91
Figura 63 – Identificación de la secuencia inicial de un mensaje DLMS/COSEM GetRequestNormal	92
Figura 64 – Decodificación en XML de un mensaje DLMS/COSEM AssociationResponse.....	92
Figura 65 – Identificación de la secuencia inicial de un mensaje DLMS/COSEM GetResponseWithDataBlock.....	93
Figura 66 – Decodificación en XML de un mensaje DLMS/COSEM AssociationResponse.....	94
Figura 67 – Identificación de la secuencia inicial de un mensaje DLMS/COSEM GetRequestForNextDataBlock.....	94
Figura 68 – Decodificación en XML de un mensaje DLMS/COSEM GetRequestForNextDataBlock.....	94
Figura 69 – Último bloque de datos perteneciente a un único mensaje DLMS/COSEM enviado por el contador	95
Figura 70 – Identificación de las secuencias iniciales de los mensajes DLMS/COSEM ReleaseRequest y ReleaseResponse	95

Figura 71 – Decodificación en XML de un mensaje DLMS/COSEM ReleaseRequest.....	96
Figura 72 – Decodificación en XML de un mensaje DLMS/COSEM ReleaseResponse	96
Figura 73 – Identificación del código OBIS en la trama PRIME.....	96
Figura 74 – Identificación de los campos DLMS/COSEM LastBlock y BlockNumber en la trama PRIME.....	96
Figura 75 – Decodificación código OBIS informe S02	97
Figura 76 – Ventana Task scheduler de la interfaz web del concentrador	98
Figura 77 – Primera solicitud de informe S05.....	98
Figura 78 – Decodificación GetRequest informe S05.....	99
Figura 79 – Decodificación código OBIS de informe S05.....	99
Figura 80 – Informe S11.....	100
Figura 81 – Informe G02	101
Figura 82 – Topología de red en bus	105
Figura 83 – Topología de red en estrella	105
Figura 84 – Captura Wireshark de solicitud y envío de informe S24	105
Figura 85 – Captura Wireshark de final de envío de informe S24	106
Figura 86 – Vista Wireshark en hexadecimal y ASCII de la primera trama enviada del informe S24	106
Figura 87 – Vista del informe S24 en IRIS	106
Figura 88 – Vista de un contador huérfano en IRIS	108
Figura 89 – Información de concentrador recién añadido a IRIS.....	108
Figura 90 – Identificación de la secuencia inicial de los mensajes SetRequestNormal y SetResponseNormal	109
Figura 91 – Decodificación SetRequestNormal	110
Figura 92 – Decodificación SetResponseNormal.....	110
Figura 93 – Geolocalización del concentrador y sus contadores asociados.....	113
Figura 94 – Pestaña “Concentradores”	139
Figura 95 – Acciones de concentrador	140
Figura 96 – Informes de concentrador.....	140
Figura 97 – Operaciones de concentrador	141
Figura 98 – Propiedades del concentrador	142
Figura 99 – Añadir atributo a un concentrador.....	143
Figura 100 – Añadir atributo libre	143
Figura 101 – Operaciones del concentrador seleccionado	144
Figura 102 – Estadísticas del concentrador	146
Figura 103 – Histórico de ping del concentrador	147
Figura 104 – Geolocalización del concentrador y sus contadores asociados.....	148
Figura 105 – Contadores asociados a un concentrador	149
Figura 106 – Propiedades del contador	149
Figura 107 – Perfiles de carga horarios por intervalo de tiempo del contador.....	150
Figura 108 – Perfiles de carga horarios por intervalo de tiempo del contador.....	151
Figura 109 – Valores diarios de consumo del contador	152

Figura 110 – Valores de consumo mensuales del contador.....	153
Figura 111 – Operaciones del contador	154
Figura 112 – Histórico de estados PLC del contador	155
Figura 113 – Histórico de potencia máxima del contador.....	155
Figura 114 – Colecciones en IRIS	156
Figura 115 – Añadir colección de usuario.....	157
Figura 116 – Borrar colección de usuario	157
Figura 117 – Información de colección de usuario	157
Figura 118 – Añadir dispositivos a una colección de usuario	158
Figura 119 – Pestaña “Firmware”	159
Figura 120 – Gestión de firmwares	159
Figura 121 – Pestaña “Sistema”	159
Figura 122 – Operaciones del sistema.....	160
Figura 123 – Estadísticas del sistema	161
Figura 124 – Valores de potencia actuales en el sistema	161
Figura 125 – Conexión de ZIV PRIME Manager	162
Figura 126 – Información del sniffer ZPM	163
Figura 127 – Captura de MAC PDUs.....	163
Figura 128 – Tráfico capturado	164
Figura 129 – Pasos para mostrar la constelación.....	164
Figura 130 – Constelación de la modulación utilizada por PRIME.....	165
Figura 131 – Pasos para mostrar el rango de frecuencias.....	165
Figura 132 – Rango de frecuencias de PRIME	166
Figura 133 – Rango de frecuencias de PRIME en media y con máximo mantenido	166
Figura 134 – Informes del concentrador ZIV	167
Figura 135 – Lista de contadores del concentrador ZIV	168
Figura 136 – Informes de contador	168
Figura 137 – Opciones del informe de contador	169
Figura 138 – Informe de contador finalizado	169
Figura 139 – Dispositivos de la subred	170
Figura 140 – Información de un nodo de la subred.....	170
Figura 141 – Planificador de tareas	171

Índice de tablas

Tabla 1 – Tipos de paquetes de control [8]	39
Tabla 2 – Tipos de paquetes de control REG [8]	40
Tabla 3 – Tipos de paquetes de control CON [8]	40
Tabla 4 – Tipos de paquetes de control PRO [8]	41
Tabla 5 – Tipos de paquetes de control BSI [8]	41
Tabla 6 – Tipos de paquetes de control FRA [8]	41
Tabla 7 – Tipos de paquetes de control ALV [8]	42
Tabla 8 – Tipos de paquetes de control MUL [8]	42
Tabla 9 – Tipos de paquetes de control PRM [8]	42
Tabla 10 – Posibles valores del campo ALV.TIME [8]	47
Tabla 11 – Posibles valores del campo ALV.TIME [8]	81
Tabla 12 – Costes materiales	117
Tabla 13 – Costes recursos humanos	118
Tabla 14 – Costes totales	118

Acrónimos

AES	<i>Advanced Encryption Standard</i>
AMI	<i>Advanced Metering Infrastructure</i>
APDU	<i>Application Protocol Data Unit</i>
ARQ	<i>Automatic Repeat reQuest</i>
BPDU	<i>Beacon PDU</i>
BSI	<i>Beacon Slot Information</i>
CENELEC	<i>Comité Européen de Normalisation ELECtrotechnique</i>
CFP	<i>Contention Free Period</i>
CID	<i>Connection Identifier</i>
CNC	<i>Concentrador</i>
COSEM	<i>COmpanion Specification for Energy Metering</i>
CRC	<i>Cyclic Redundancy Check</i>
CSMA/CA	<i>Carrier Sense Multiple Access with Collision Avoidance</i>
D8PSK	<i>Differential Eight-Phase Shift Keying</i>
DBPSK	<i>Differential Binary Phase Shift Keying</i>
DLMS	<i>Device Language Message Specification</i>
DPSK	<i>Differential Phase Shift Keying</i>
DQPSK	<i>Differential Quaternary Phase Shift Keying</i>
DSO	<i>Distribution System Operator</i>
EUI-48	<i>48-bit Extended Unique Identifier</i>
FEC	<i>Forward Error Correction</i>
FTP	<i>File Transfer Protocol</i>
HTTP	<i>HyperText Transfer Protocol</i>
ICT	<i>Information and Communication Technologies</i>
IEEE	<i>Institute of Electrical and Electronics Engineers</i>
IP	<i>Internet Protocol</i>
ITU-T	<i>Telecommunication Standardization Sector of the International Telecommunications Union</i>
LCID	<i>Local Connection IDentifier</i>
LLC	<i>Logical Link Control</i>
LNID	<i>Local Node IDentifier</i>
LSID	<i>Local Switch IDentifier</i>
MAC	<i>Medium Access Control</i>
MDMS	<i>Meter Data Management System</i>
MTU	<i>Maximum Transmission Unit</i>
M2M	<i>Machine-to-Machine</i>
NB-PLC	<i>Narrowband Power Line Communications</i>
NID	<i>Node Identifier</i>
OBIS	<i>Object Identification System</i>
OFDM	<i>Orthogonal Frequency Division Multiplexing</i>
OSGP	<i>Open Smart Grid Protocol</i>

OSIRIS	Optimización de la Supervisión Inteligente de la Red de Distribución
PDU	<i>Packet Data Unit</i>
PHY	<i>Physical Layer</i>
PLC	<i>Power Line Communications</i>
PNPDU	<i>Promotion Needed PDU</i>
PRIME	<i>PoweRline Intelligent Metering Evolution</i>
SCP	<i>Shared Contention Period</i>
SDU	<i>Service Data Unit</i>
SID	<i>Switch Identifier</i>
SMTP	<i>Simple Mail Transfer Protocol</i>
SNA	<i>SubNetwork Address</i>
SOAP	<i>Simple Object Access Protocol</i>
STG-DC	Sistema de Telegestión – <i>Data Concentrator</i>
TCP	<i>Transmission Control Protocol</i>
TFG	Trabajo de Fin de Grado
TIC	Tecnologías de la Información y la Comunicación
UDP	<i>User Datagram Protocol</i>
WS	<i>Windows Size</i>
XML	<i>Extensible Markup Language</i>

Capítulo 1

Introduction

This chapter provides an overview of the TFG, including an introduction to the PLC communication technology, focusing on PRIME protocol. It sets out the reasons that have led to the realization of this TFG, the objectives to be achieved with it and the structure followed by this document.

1.1 Motivation

Nowadays, technology is everywhere, it accompanies us wherever we go and is present in the daily lives of the vast majority of the population. It is impossible to quantify the huge impact that technological development has had on the life of the human being, to the point that both social and economic development are not currently understood if they do not go along with it. Technology has changed the way we work, transport and even communicate.

In an increasingly complex and interconnected society, it is difficult to think of a sector in which Information and Communication Technologies (ICT) are not present, and the energy sector is no exception. ICT development is being key for this sector, which seeks to respond to the new needs of customers by promoting a more flexible and efficient management of networks through the so-called Smart Grids. Smart Grids are those ones which are capable of integrating the behavior and actions of all customers connected to it in an agile and efficient way, including a wide variety of operational and energy measures and ensuring a more sustainable and efficient power grid with low losses and high quality and safety levels [1].

Smart Grids represent a real revolution, since they are systems that allow bidirectional communication between the customer and the public utility company, so that the latter can store the information provided by the former in order to improve the management of its network. In addition, with the growing presence of renewable energies we face the scenario that the customer is not only an energy consumer, but also a producer. It is therefore important that this networks facilitate the progressive incorporation of such renewable energies taking into account their particularities and limitations.

The M2M (Machine-to-Machine) communications concept, which refers to data exchange between two remote machines, is particularly important in Smart Grids, since they allow the bidirectional exchange of information in real time between the managed and monitored devices and the data storage and processing systems. Among the devices that use M2M communications stand out the AMI (Advanced Metering Infrastructure), including smart meters which communicate with public utility systems. On the other hand, the recent advances in data processing and management, with the emerging big data leading the way, are particularly relevant since they will make it possible to manage and process data in order to make decisions based on this large amount of information [2].

According to the annual report of 2015 conducted by EURELECTRIC [3], the sector association which represents the common interests of the electricity industry at a European level, electricity companies throughout next ten years are expected to invest 350 billion euros in the deployment of Smart Grids for around 260 million customers.

The European Directive 2009/72/EC [4] included means to protect consumers, including the obligation of Member States to ensure the use of smart meters.

In Spain, the progressive implementation of this type of meters has been planned since 2007. In this year, the Royal Decree 1110/2007 [5], which establishes the necessary functionalities of remote management systems and also the requirements to be met by metering equipment, was approved, and the Order ITC/3860/2007 [6] which details the “Meter replacement plan” and establishes the deadline for its total implementation in Spain on December 31, 2018.

Among the different methods that can be considered for the transmission of information in Smart Grids, PLC (Power Line Communications) technology is very interesting for direct communication with Smart Meters in the so-called last mile of the Advanced Metering Infrastructures due to the use of existing electric infrastructure (electrical wiring) as a communication medium. The use of PLC technology is particularly interesting for the electrical distributors (DSO or Distribution System Operator), since it does not require the deployment of new infrastructures for communications. Because power cables are not intended to be used as a communication medium, they offer a rather hostile environment from the point of view of data transmission, due to factors such as noise or impedance variation. Despite this, PLC offer many valuable advantages to DSOs, especially Narrowband PLS (NB-PLC), whose standards were developed to mitigate some of the problems in PLC communications. Currently, these NB-PLC standards are being widely used for communication between Smart Meters and data concentrators in AMI deployments [7].

At present, there are different NB-PLC standards, being PRIME (PowerLine Intelligent Metering Evolution) and Meters & More the most widely used in Spain. PRIME technology, as mentioned, is widely deployed in Spain and represents a mature standard with international projection and used by some of the largest DSOs in Spain like Iberdrola and Fenosa.

PRIME standard is promoted by the PRIME Alliance, led by Iberdrola, and is a free, open and not subject to intellectual property rights. Due to this fact, it makes it easy that new entrants can provide interoperable solutions. Its aim is to provide a standard among equipment and systems from different vendors [8].

Along with PRIME, new communication protocols are designed to enable the transmission of information between different elements of Smart Grids. One of these protocols is DLMS/COSEM (IEC 62056), application layer protocol designed specifically for communication with Smart Meters. DLMS (Distribution Line Message Specification) is the PRIME application layer protocol and supports functions such as remote meter reading, remote control and value-added services to measure any type of energy. COSEM (Companion Specification for Energy Metering) is the data model used for communication between measuring equipment.

Smart Grids deployment also has one of its main attractions in the possibility that DSOs can remotely manage their power grid. Due to this fact, different platforms and Smart Grids remote management systems that provide the necessary functionalities for grid management have emerged, as well as a wide range of statistics to know in detail the state of the different elements of the grid in real time. STG-DC protocol, based on web services, is defined for the communication between these remote management platforms (STG or *Sistema de TeleGestión*) and the data concentrators (DC). The PRIME meters and concentrators remote management platform to be used and analyzed in this TFG is IRIS, intended for commercial use and developed by STM Telecontrol.

The research group of the Telematics Engineering Department in which this TFG has been developed is framed within the OSIRIS project (*Optimización de la Supervisión Inteligente de la Red de Distribución*) [9], financed by the Ministry of Economy and Competitiveness and led by Union Fenosa Distribución (third national electricity distributor). For this research group a cyber-physical infrastructure fully manageable from IRIS is available. This infrastructure is composed of both physical and virtual devices. In the physical part, there are four smart meters, all of them of ZIV brand, associated to a data concentrator also from ZIV. The virtual part of the infrastructure is larger and can give an idea of the number of devices that a DSO may have to remotely manage. This virtual infrastructure consists of ten concentrators, each with a number of associated meters ranging from 150 to 170.

Because both the concept of Smart Grid and the different technologies involved in its deployment are relatively recent, the training of qualified professionals in this field is still at an early stage, both at the corporate and academic levels. However, the energy sector revolution brought about by the development of Smart Grids and the prospects for the future that are envisaged around them are leading to a growing demand for this type of professionals.

Motivated by these growing needs in the field of Smart Grids, this TFG arises with the purpose of bringing the student closer to these ever more present future networks. It will deal with aspects of different segments of a Smart Grid, from the communication between devices to its remote management through IRIS, in order to analyze the potential of the available cyber-physical infrastructure.

1.2 Goals

The main goal of this TFG is to develop a battery of tests that illustrates the functionality and potential of the available cyber-physical infrastructure. This set of tests will be raised from a teaching point of view, for its use in the academic field. Therefore, this practice manual can be used in future subjects in order to train professionals in the competences related to the field of Smart Grids.

In order to reach this final goal, a series of intermediate steps or sub-goals which will guide this TFG have been defined:

- Analysis of the state of the art of the different technologies involved in PRIME networks and that are relevant to this TFG.
- Documentation of the use of the different tools that need to be used to achieve the main objective.
- Elaboration of a practice manual with a set of tests that allow a thorough analysis of the available cyber-physical infrastructure potential and functionality.
- Elaboration of a solution of the mentioned practice manual that include each individual solution and in which the methodology to follow to carry out each single test is defined, as well as the analysis of the obtained results, including the corresponding illustrative material.
- Accurate documentation of all the process carried out.

1.3 Memory structure

This TFG is intended to serve as a guide for potential labs, so it includes all the necessary information for this purpose, from the summaries of the communication protocols to the manuals of the involved tools. It is essential to provide future users with all the necessary information to prepare a lab manual aimed to be a part of the course syllabus so that this manual can be as complete as possible. This explains the final length of the memory, which is significantly higher than the recommended one. However, the main contribution of this TFG is the definition of the battery of tests along with its corresponding solution (Chapters 3 and 4). The rest of the sections can be consulted by the reader to allow him to expand knowledge or understand other parts of the project.

This TFG is organized in different chapters that cover each of the phases of its realization. The structure and content are detailed below:

- **Chapter 1: Introduction**

This chapter provides an overview of the TFG, including an introduction to the PLC communication technology, focusing on PRIME standard. It sets out the reasons that have led to the realization of this TFG, the objectives to be achieved with it and the structure of this document.

- **Chapter 2: State of the art**

This chapter analyzes the state of the art of the different technologies related to this TFG and that take part in the deployment of AMI, focusing mainly on PRIME and other related protocols, and on the tools used during the development of this project. In addition, the cyber-physical infrastructure is presented in detail. Finally, the regulatory framework applicable at both national and European level is set out.

- **Chapter 3: Design**

This chapter describes the requirements and restrictions for the preparation of the lab manual. After defining these points, the manual, composed by the battery of tests to be carried out on the cyber-physical infrastructure, is presented. The tests are designed to make use of the tools described in **Chapter 2** and to test the knowledge about the involved technologies with the ultimate goal of illustrating and analyzing the potential of the cyber-physical infrastructure.

- **Chapter 4: Results and evaluation**

This chapter details the results of the different tests carried out on the cyber-physical infrastructure, in order to give a clear view about its potential. For this purpose, each test result is analyzed in a clear and illustrative way.

- **Chapter 5: Socio-economic impact**

In this chapter, the socio-economic implications of this TFG are presented. It analyses the impact of this project taking into account the current energetic context in Spain and presents the planning followed for its realization along with its budget.

- **Chapter 6: Conclusions**

In this last chapter of the TFG, the conclusions obtained after the completion of this project, as well as the knowledge acquired during its realization and future lines of research, are set out.

- **ANNEXES**

- **Annex 1:** Extended Abstract
- **Annex 2:** STG-DC reports and orders.
- **Annex 3:** IRIS user manual.
- **Annex 4:** ZIV PRIME Manager user manual.
- **Annex 5:** ZIV Concentrator web interface user manual

Capítulo 2

Estado del arte

En este capítulo se analiza el estado del arte de las diferentes tecnologías que influyen en el despliegue de AMI, centrándose sobre todo en PRIME. Además, se presentan en detalle la infraestructura ciber-física y las herramientas de las que se dispone y se resume el marco regulatorio, tanto a nivel nacional como europeo, aplicable a este proyecto.

2.1 Arquitectura de comunicaciones para AMI

La **Figura 1** muestra una visión global de una arquitectura de comunicaciones típica para AMI. Como puede verse, los principales dispositivos y sistemas involucrados son: contadores, concentradores de datos y sistemas de información. Estos dispositivos están organizados jerárquicamente, controlando cada concentrador las comunicaciones con un conjunto de contadores, mientras el sistema de información tiene una visión completa de la infraestructura.

Además, suele tratarse de infraestructuras de comunicaciones heterogéneas, que involucran diferentes tecnologías dependiendo de los requisitos específicos de cada segmento de red. Como también muestra la **Figura 1**, en España la comunicación entre los contadores y el concentrador de datos está basada en tecnologías PLC de banda estrecha, como PRIME o Meters & More. Estos protocolos PLC de banda estrecha abarcan la capa física (PHY), la capa de enlace de datos (*Data Link Layer*) y la capa de convergencia (*Convergence Layer* – CS). A nivel de aplicación se utiliza el protocolo DLMS/COSEM. Para la comunicación entre el concentrador y el sistema de información se suelen utilizar tecnologías de banda ancha y largo alcance, como tecnologías celulares (típicamente GPRS) o medios cableados (típicamente Fibra Óptica). En este segmento de red, en el caso de PRIME, a nivel de aplicación se utiliza STG-DC, una especificación de la *PRIME Alliance* basada en servicios web.

A continuación, se estudian en detalle las tecnologías y protocolos específicos de AMI mostrados en la **Figura 1**.

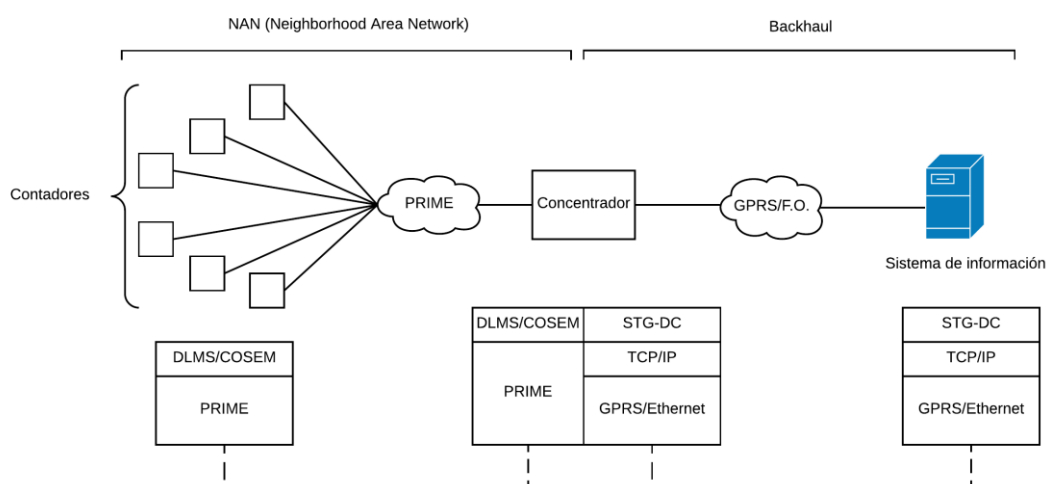


Figura 1 – Arquitectura de comunicaciones típica para Sistemas de Medición Avanzada

2.2 Visión global de las tecnologías PLC de Banda Estrecha

En la actualidad existe una amplia variedad de tecnologías para la comunicación entre dispositivos de una *Smart Grid*. Esta comunicación se puede llevar a cabo mediante PLC, a través de una red pública de comunicaciones (GPRS, GSM, DSL o fibra óptica), o mediante otras tecnologías como ZigBee o WiMAX [10].

De todas estas posibilidades, la tecnología PLC de banda estrecha (NB-PLC) es la más apropiada en la última milla para la comunicación entre los concentradores de datos y los contadores inteligentes debido, sobre todo, a que es la que ofrece un menor coste de infraestructura ya que las líneas ya están desplegadas. Otra ventaja que ofrece el uso de PLC es que hace posible la comunicación de dos equipos de distintas instalaciones solamente mediante la conexión a la toma de corriente. Sin embargo, la tecnología PLC también presenta ciertos problemas, ya que el medio utilizado no fue diseñado para la transmisión de datos, como las interferencias electromagnéticas, el ruido o la variación de la impedancia del canal. El uso de tecnología NB-PLC consigue mitigar en parte algunos de estos problemas propios del medio [11].

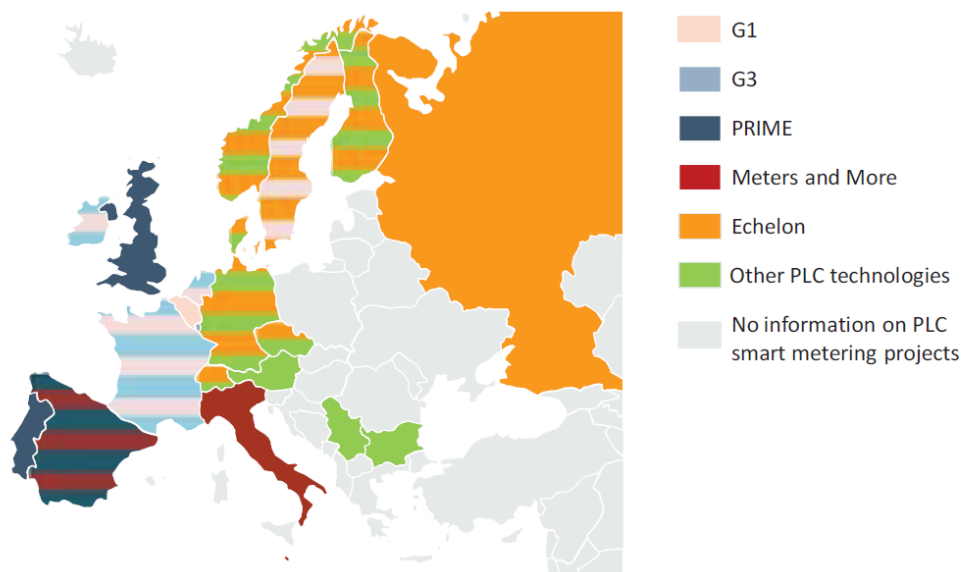


Figura 2 – Despliegue de tecnologías NB-PLC en Europa [12]

Existen diferentes estándares NB-PLC en el mercado europeo, que cuentan con diferentes grados de penetración según la zona geográfica, como se puede ver en la **Figura 2**. Los principales estándares en NB-PLC en la actualidad son los siguientes:

- *Meters and More* es una tecnología liderada por el grupo Enel cuyas capas inferiores han sido aceptadas como estándar por IEC/CENELEC (CLC TS 50568-4). Su mayor grado de penetración se da en los países donde opera el grupo Enel, como Italia, de donde es originario dicho grupo y donde el 100% de los contadores inteligentes utilizan esta tecnología, o España donde a partir de 2018 la utilizarán aproximadamente el 50% de los contadores (actualmente Endesa es propiedad en un 70% del grupo Enel). Funciona en la banda CENELEC-A (3-95 KHz). Utiliza una única portadora y ofrece una gran robustez, aunque sus tasas de transmisión son bajas (9.6 kbps).
- *Open Smart Grid Protocol* (OSGP) es una familia de especificaciones promovida por el grupo norteamericano Echelon. Aunque sus capas inferiores están también estandarizadas por el IEC (IEC 14908.1). Sus mayores niveles de penetración se dan en los países nórdicos y Rusia. Funciona en la banda CENELEC-A y utiliza una única portadora, ofreciendo bajas tasas de transmisión (hasta 3.6 kbps).
- CX1 es una tecnología promovida por Siemens cuyas capas inferiores están siendo estandarizadas por el IEC/CENELEC (CLC TS 50590). Su despliegue en la actualidad se limita a Austria. Funciona en la banda CENELEC-A. Se trata de una tecnología que utiliza modulación multiportadora adaptativa, lo que le permite alcanzar tasas de hasta 64 kbps.
- G3 es una tecnología cuya especificación lidera la distribuidora francesa EDF en colaboración con el fabricante de chipsets Maxim (miembros de la G3-PLC Alliance), aunque sus capas PHY y de enlace han sido publicadas como estándar por la ITU-T (ITU-T G.9903 [13]). Registra sus mayores índices de presencia en países donde opera EDF (sobre todo Francia). Aunque se diseñó inicialmente para trabajar en la banda CENELEC-A, recientemente ha sido extendida para poder trabajar en el mercado americano (FCC) y asiático (ARIB). Es una tecnología multiportadora, que destaca por ofrecer una gran robustez y que ofrece tasas de hasta 34 kbps.
- *PowerLine Intelligent Metering Evolution* (PRIME), como ya se ha mencionado, es una tecnología promovida por la PRIME Alliance liderada por algunas de las distribuidoras españolas más importantes, como Iberdrola o Unión Fenosa Distribución y por fabricantes de chipsets como Texas Instruments. Sus capas PHY y de enlace han sido publicadas como estándar por la ITU-T (ITU-T G.9904 [8]). Fue inicialmente diseñada para funcionar en la banda CENELEC-A, pero, al igual que G3, ha sido extendida para ser utilizada en el mercado americano y asiático. Se trata de una tecnología multiportadora que ofrece tasas de hasta 128.6 kbps.
- G.hnem es una tecnología desarrollada por la ITU-T, en colaboración con la G3-PLC Alliance y la PRIME Alliance, en su afán por armonizar estas dos tecnologías NB-PLC. Su implementación es computacionalmente más compleja y su utilización es muy baja en la actualidad.

- IEEE 1901.2 es la especificación NB-PLC del IEEE. Su utilización en la actualidad es también muy baja.

PRIME sobresale como tecnología NB-PLC ya que se trata de un estándar consolidado en España y con una gran proyección internacional (está siendo implantada en países como Reino Unido, Portugal, Polonia, Australia o Brasil). En la actualidad hay más de 10 millones de *Smart Meters* PRIME instalados en todo el mundo, de los cuales más de 5 millones se encuentran en España, cifra que se prevé que aumente hasta los 15 millones en 2018 (debido a la legislación española IET/290/2012).

La infraestructura ciber-física de la que se dispone en el grupo de investigación del Departamento de Ingeniería Telemática está formada por dispositivos (contadores inteligentes y concentradores de datos) PRIME, por lo que a partir de ahora se profundiza en esta tecnología.

2.3 PRIME

2.3.1 General

PRIME (*PoweRline Intelligent Metering Evolution*) es un estándar abierto, libre y sin propietario, definido por la PRIME Alliance [14], para una tecnología OFDM PLC disponible en el mercado que asegura verdadera interoperabilidad entre equipos y sistemas. Los componentes de la arquitectura PRIME no están sujetos a derechos de propiedad intelectual y están disponibles de manera pública, lo que facilita que nuevos entrantes puedan ofrecer soluciones interoperables al mercado. Su arquitectura ha sido diseñada de modo que se consiga un bajo coste y a la vez un alto rendimiento. La capa física, la capa MAC y la capa de convergencia de la versión 1.3.6 de la especificación están consideradas como estándar por la ITU-T desde el año 2012. La versión 1.4 amplía el espectro de frecuencias para permitir operar en los mercados norteamericano y asiático e incluye algunas mejoras encaminadas a mejorar la robustez a nivel físico y MAC.

2.3.2 Capa física

En el apartado de la capa física, PRIME opera en la banda CENELEC-A (3-95 KHz), más concretamente en la banda de 41-89 KHz en su versión 1.3.6, mientras que en su versión 1.4 opera en la banda de 3-500 KHz. Se trata de una tecnología multiportadora que utiliza multiplexación OFDM para utilizar de manera más eficiente el espectro. Los dispositivos PRIME utilizan modulación diferencial con las constelaciones DBPSK, DQPSK o D8PSK. Además, permite la utilización de FEC para la recuperación frente a errores introducidos por el canal. La velocidad de transmisión de datos en redes PRIME puede ir desde los 5.4 kbps hasta los 1028.8 kbps, dependiendo del modo de comunicación (combinación de modulación digital y FEC) [8].

2.3.3 Capa MAC

2.3.3.1 General

La capa MAC pertenece a la Capa de Enlace de Datos. A nivel MAC, una subred tiene una estructura similar a la de un árbol, donde se pueden distinguir dos tipos de nodos: el nodo base (*base node*) y los nodos de servicio (*service nodes*).

- El nodo base es único y se encuentra en la raíz de la estructura de árbol anteriormente mencionada y actúa como nodo maestro, proporcionando

conectividad al resto de elementos y gestionando los recursos y conexiones de la subred. En la terminología AMI, el nodo base es el concentrador de datos.

- Los nodos de servicio pueden ser tanto hojas como ramas del árbol e inicialmente se encuentran en estado desconectado, siendo sus funciones mantener la conectividad con subred para las diferentes capas de aplicación y conmutar la información de otros nodos. En terminología AMI los nodos de servicio son los contadores inteligentes o *smart meters*.

Inicialmente la subred está compuesta únicamente por el nodo base y el resto de nodos que pretendan formar parte de ella tienen que realizar un procedimiento de registro.

Los tres estados funcionales de un nodo de servicio son:

- Desconectado: es el estado inicial en el cual no puede transmitir ni conmutar información.
- Terminal: el nodo de servicio puede establecer conexiones y comunicar información.
- *Switch*: el nodo de servicio puede realizar todas las funciones de un nodo terminal y además puede reenviar la información de otros nodos en la misma subred.

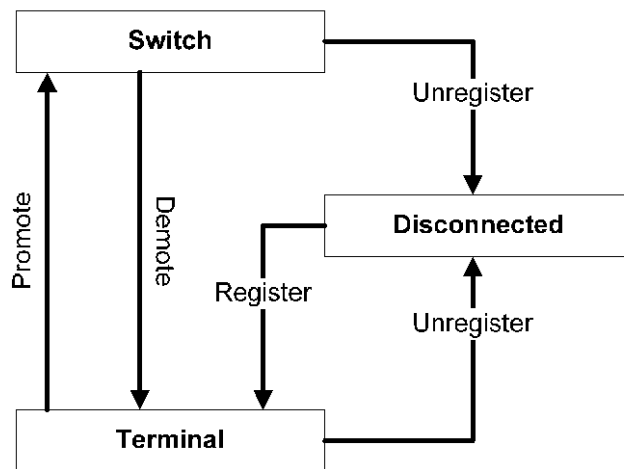


Figura 3 – Estados funcionales de un nodo de servicio [8]

El paso de un estado funcional a otro tiene lugar mediante los procesos de registro (de desconectado a terminal), anulación del registro o desregistro (el nodo de servicio pasa al estado desconectado y ya no está en la subred), promoción (nodo terminal pasa a ser nodo *switch*) y degradación (nodo *switch* pasa a ser nodo terminal).

Cada nodo tiene una dirección MAC de 48 bits llamada EUI-48, utilizada para identificarlo durante el proceso de registro. La EUI del nodo base sirve para identificar a la subred y se denomina SNA (*SubNetwork Address*). El LSID (*Local Switch Identifier*) es un identificador único de 8 bits que sirve para cada nodo *switch*. Cada nodo de

servicio recibe un identificador local de 14 bits llamado LNID (*Local Node Identifier*). El LNID y el SID (LSID del nodo *switch* al que esté asociado) forman un identificador de 22 bits denominado NID (*Node Identifier*). Durante el establecimiento de la conexión se reserva un identificador local de conexión de 9 bits (LCID) que identifica una única conexión. El NID y el LCID forman un identificador de conexión de 31 bits (CID).

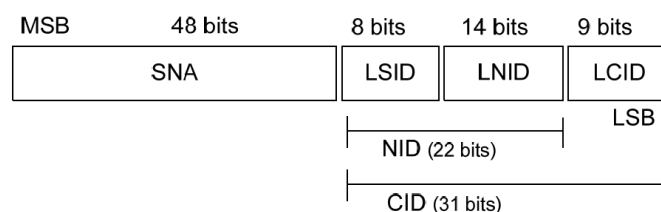


Figura 4 – Estructura de direccionamiento [8]

La asignación de direcciones se realiza según el proceso que se detalla a continuación:

En un principio en la subred sólo está el nodo base con NID = (0,0), por ejemplo (LNID=SID, LNID), estando todos los nodos de servicio en estado desconectado. El resto de nodos pretenden registrarse en la red, pero solo podrán hacerlo los que se encuentren en el nivel inmediatamente inferior al nodo base (nivel 0). Después de que se produzca el registro de estos nodos se les asigna como SID el LSID del nodo base (0 en este caso), ya que es el nodo *switch* del que dependen, y un LNID único para cada uno de ellos.

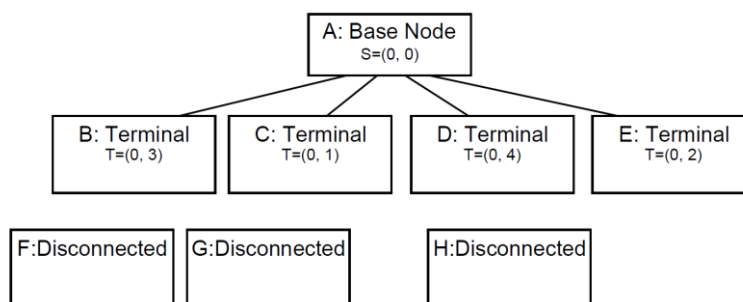


Figura 5 – Asignación de direcciones: fase 1 [8]

Los nodos de servicio del siguiente nivel (nivel 1) no pueden conectarse al nodo base, que es el único nodo *switch* en la subred, por lo que necesitarán que se realice una promoción de ciertos nodos de servicio del nivel 0 (tras el registro son todos nodos terminales), para lo que enviarán un broadcast de solicitudes PNPDU (*Promotion Needed PDU*). Los nodos del nivel 0 que acepten esta solicitud a su vez realizarán una solicitud de promoción al nodo base para extender la subred. Durante la promoción, a estos nodos de servicio se les asignará un SID único para las funciones de *switching*, manteniendo también el asignado durante el registro para la comunicación como nodo terminal.

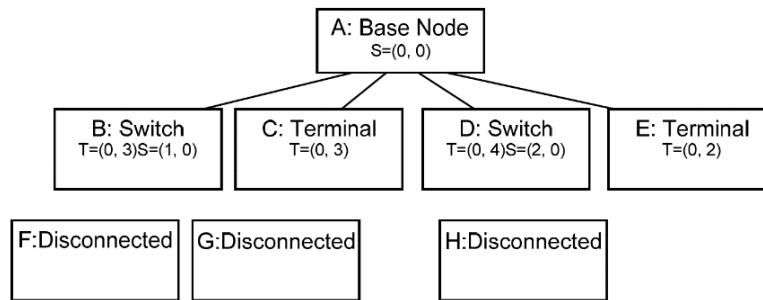


Figura 6 – Asignación de direcciones: fase 2 [8]

Cuando el proceso de promoción termina, los nodos que quieren acceder a la subred inician su proceso de registro, donde se les asigna el SID (LSID del nodo *switch* del que dependa cada uno) y un LNID único (dentro del conjunto de nodos que dependen del mismo nodo *switch*).

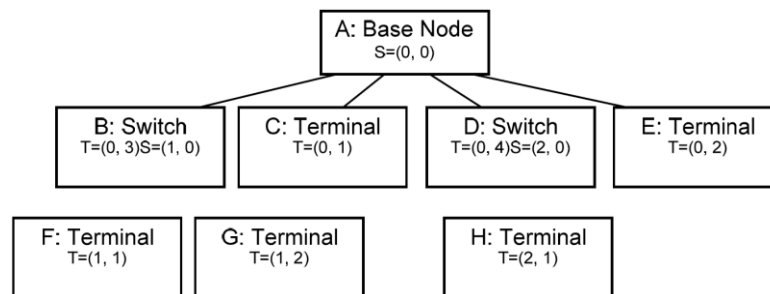


Figura 7 – Asignación de direcciones: fase 3 [8]

Los paquetes transmitidos pueden tener las siguientes direcciones de destino:

- LNID=0x3FFF → Broadcast (los paquetes llegan a todos los nodos de la subred)
- LNID=0x3FFE → Multicast (los paquetes llegan a un grupo de nodos definido por el LCID)
- LNID=resto → Unicast (el paquete se envía al nodo con este LNID)

2.3.3.2 Creación y mantenimiento de subredes

El nodo base es el encargado de la creación de la subred y de su mantenimiento. Las acciones que realiza el nodo base para el mantenimiento de la subred son las siguientes:

- Transmisión de balizas. El nodo base debe transmitir exactamente una baliza por trama, mientras que los nodos *switch* transmiten balizas con una frecuencia determinada por el nodo base.
- Promoción y degradación de nodos terminales y *switch*. Todas las solicitudes de promoción se dirigen al nodo base, que tiene una tabla con todos los nodos *switch* de la subred y asigna un SID único a las nuevas solicitudes aceptadas. La

degradación puede ser iniciada por el propio nodo base o ser solicitada por el nodo *switch* en cuestión.

- Gestión de registros. El nodo base recibe todas las solicitudes de registro y decide si aceptarlas o rechazarlas. En caso de aceptar una solicitud, asigna un NID (SID+LNID) único para ella.
- Configuración y gestión de la conexión. El nodo base actúa en todas las conexiones de la subred, ya sea como parte de esta conexión o como gestor.
- Arbitraje de acceso al canal. El nodo base decide qué dispositivos utilizarán el canal y con qué mecanismos.
- Distribución de secuencias aleatorias para obtener la clave de cifrado. La clave de cifrado se obtiene a partir de una secuencia aleatoria de 128 bits. El nodo base debe generar periódicamente una nueva secuencia y distribuirla a toda la subred.
- Gestión de grupos multicast: El nodo base debe mantener todos los grupos multicast, gestionando todas las altas y bajas dentro de estos.

2.3.3.3 Acceso al canal

Existen ciertas directrices para el acceso al canal de los dispositivos de una subred. El tiempo está dividido en tramas MAC. Los nodos de servicio y el nodo base pueden acceder al canal en el periodo con contienda o SCP (Shared-Contention Period) o solicitar un periodo libre de contienda o CFP (Contention-Free Period).

El acceso CFP deber ser solicitado por el dispositivo y asignado por el nodo base, que puede conceder acceso a dicho dispositivo para una duración específica o denegar la solicitud. En la actualidad, el CFP no está implementado por los fabricantes.

El acceso SCP no requiere de arbitraje, pero los dispositivos deben respetar los límites de tiempo SCP en una trama MAC. El SCP es el tiempo en el que cualquiera de los dispositivos de la subred puede transmitir información. La longitud del SCP puede variar de una trama a otra y se indica mediante información en la baliza. Para evitar colisiones en el acceso al medio mediante SCP se utiliza CSMA/CA como técnica de acceso.

Una trama MAC está compuesta por una o más balizas, un SCP y un CFP o ninguno.

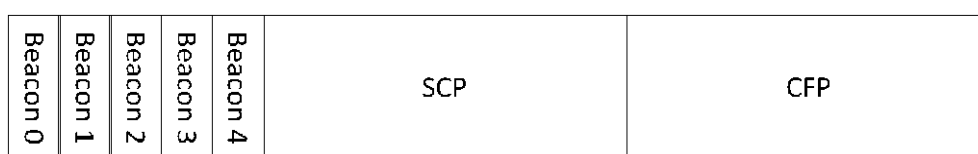


Figura 8 – Estructura de una trama MAC [8]

El nodo base transmite una BPDU (Beacon PDU) en cada trama MAC. Los nodos *switch* también transmiten BPDUs para mantener la parte de la subred que depende de cada uno de ellos. La transmisión de BPDUs por parte de los nodos *switch* se realiza en intervalos de tiempo regulares, pero no necesariamente iguales que el del nodo base ya que un nodo *switch* no tiene por qué enviar su BPDU en cada trama MAC.

La unidad de tiempo en la que se transmite un BPDU se denomina *beacon slot* (ranura de baliza). El primer slot de cada trama está reservado para el nodo base. El número de slots en cada trama puede variar y es indicado por el nodo base mediante su BPDU. Cuando se registra un nuevo *switch* en la subred, aumentará el número de slots y el nodo base puede cambiar los slots y la frecuencia de transmisión de dispositivos *switch* ya registrados. Cuando esto ocurre el nodo base envía un paquete de control BSI (Beacon Slot Information) para cada *switch* afectado y este responde con un ACK. Si se produce un cambio en el número de *beacon slots* durante su reorganización, el nodo base debe transmitir un paquete de control FRA a toda la subred indicando cambio en la estructura de la trama. Los dispositivos *switch* que reciben tanto paquetes BSI como FRA deben retransmitirlos a todos los dispositivos de su dominio.

2.3.3.4 Conmutación (*switching*)

El nodo base de una subred no puede comunicarse directamente con todos los nodos. Los nodos *switch* retransmiten tráfico desde/hacia el nodo base de manera que cualquiera de los nodos de la subred se puede comunicar con el nodo base.

Cada *switch* mantiene una tabla de los demás nodos *switch* conectados en la subred a través de él. Esta tabla se denomina tabla de *switching*. Para reenviar la información no es necesaria más información, ya que el tráfico desde/hacia los nodos terminales contiene información de sus respectivos nodos *switch*.

Inicialmente, la tabla de *switching* de los nodos *switch* está vacía y es actualizada mediante un seguimiento de las promociones y degradaciones de otros nodos. Con cada ACK de promoción (PRO_ACK) se crea una nueva entrada en la tabla. Cuando se recibe una solicitud de degradación (PRO_DEM_x), la entrada correspondiente al NSID de dicho nodo es eliminada de la tabla.

A continuación, se muestra un ejemplo de tablas de *switching*:

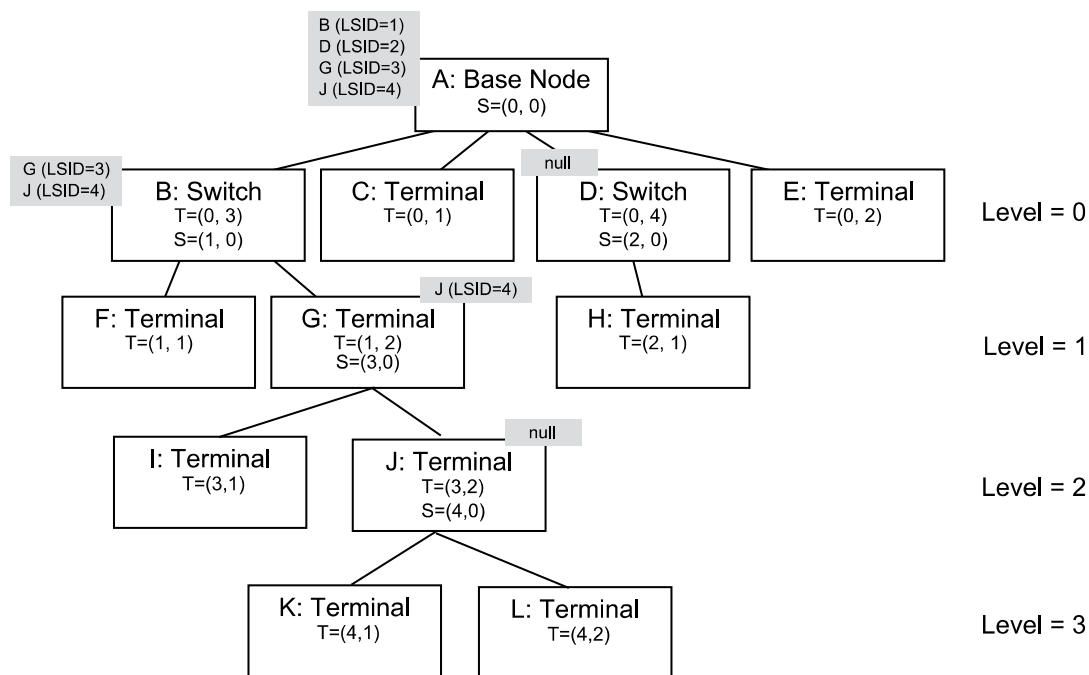


Figura 9 – Ejemplo de tablas de switching [8]

2.3.3.5 Seguridad

Para conseguir una conexión segura, la capa MAC de PRIME cuenta con medidas de seguridad que garantizan privacidad, autenticación e integridad de datos, así como una política de gestión de claves. Todos los paquetes deben ajustarse al perfil de seguridad, excepto los mensajes de control REG y SEC, y las BPDU que se transmitan sin encriptación. Existen dos perfiles de seguridad dependiendo de las necesidades de seguridad: perfil de seguridad 0 y perfil de seguridad 1.

▪ Perfil de seguridad 0

El perfil de seguridad 0 es utilizado en las comunicaciones orientadas a la transmisión de MAC SDUs (*Service Data Units*) sin encriptar. Este perfil puede ser utilizado cuando la seguridad no es demasiado importante, o cuando es suficiente con la proporcionada por capas superiores.

▪ Perfil de seguridad 1

El perfil de seguridad 1 está basado en el cifrado de datos AES de 128 bits y su CRC asociado. Este perfil está diseñado para cumplir con todos los requisitos de seguridad: privacidad, autenticación e integridad de datos. La privacidad se garantiza mediante el cifrado y por el hecho de que la clave de cifrado es secreta. La autenticación se garantiza por el hecho de que cada nodo tiene su propia clave secreta, conocida sólo por el propio nodo y por el nodo base. La integridad de los datos se garantiza debido a que el CRC del payload está cifrado.

El algoritmo criptográfico utilizado es AES (*Advanced Encryption Standard*) y es utilizado de acuerdo al llamado ECB, que es un modo de cifrado de bloques en el que el texto sin formato se divide en bloques de 128 bits.

$$\text{Generated Key} = \text{AES_enc}(\text{Generation Key}, \text{Constant})$$

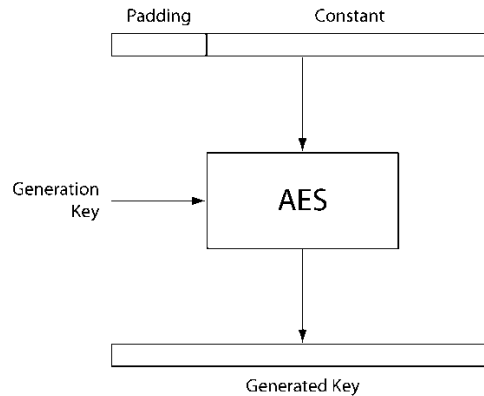


Figura 10 – Algoritmo de encriptación AES [8]

Todos los datos en la capa MAC utilizan el mismo perfil de seguridad. Este perfil es negociado durante el registro del dispositivo. En el mensaje de solicitud de registro (REG_REQ) el dispositivo indica un perfil de seguridad en el campo REG.SPC. Este perfil debe ser aceptado por el nodo base en el mensaje REG_RSP con el mismo valor de REG.SPC.

2.3.3.6 Formatos de MAC PDUs

2.3.3.6.1 MAC PDU Genérica

Las GPDU (Generic MAC Packet Data Units) son utilizadas para el tráfico de datos y la mayoría del tráfico de control. Todos los paquetes de control MAC son transmitidos como GPDU. Una MAC PDU Genérica está formada por la cabecera (3 bytes), uno o varios paquetes y el CRC (4 bytes):

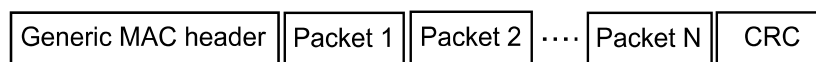


Figura 11 – Estructura de una GPDU [8]

Como se aprecia en la **Figura 11**, una MAC PDU Genérica puede transportar más de un paquete. Esto se consigue mediante la funcionalidad denominada agregación de paquetes. En el ámbito de este Trabajo de Fin de Grado no se utilizará agregación de paquetes, por lo que cada GPDU contendrá un único paquete.

La cabecera de una MAC PDU tiene los siguientes campos:

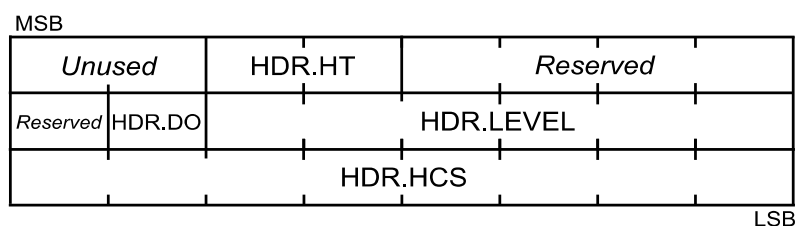


Figura 12 – Campos de la cabecera de una GPDU [8]

- Unused → 2 bits.
- HDR.HT → 2 bits; HDR.HT = 0 para GPDU.
- Reserved → 5 bits; siempre 0.
- HDR.DO → 1 bit; valor 1 cuando la MAC PDU está en el enlace descendente y valor 0 para el enlace ascendente.
- HDR_LEVEL → 6 bits; nivel de la PDU en la jerarquía de switching.
- HDR.HCS → 8 bits; secuencia para detectar errores en la cabecera y comprobar que la MAC PDU pertenece a la subred.

Un paquete está formado por cabecera (6 bytes) y carga útil o payload:

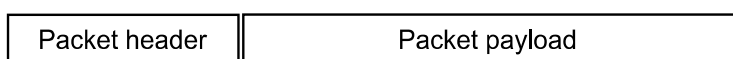


Figura 13 – Estructura de un paquete [8]

La cabecera de un paquete tiene los siguientes campos:

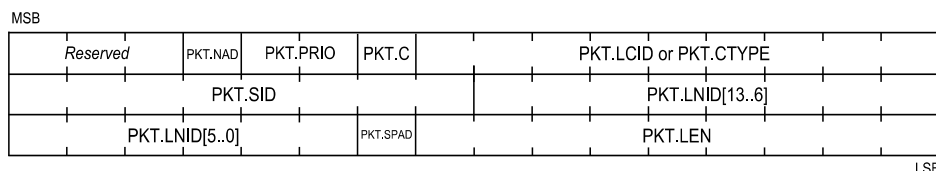


Figura 14 – Campos de la cabecera de un paquete [8]

- Reserved → 3 bits; siempre 0
- PKT.NAD → 1 bit; 0 si puede ser agregado con otros paquetes en el destino, 1 si no.
- PKT.PRIO → 2 bits; prioridad entre 1 y 3.
- PKT.C → 1 bit; 0 si es un paquete de datos, 1 si es un paquete de control.
- PKT.LCID/PKT.CTYPE → 9 bits; dependiendo del valor de PKT.C, PKT.LCID es el id. local de conexión de un paquete de datos y PKT.CTYPE indica el tipo de paquete de control.
- PKT.SID → 8 bits; si HDR.DO = 0 representa el SID del origen, si HDR.DO = 1 representa el SID del destino.
- PKT.LNID → 14 bits; si HDR.DO = 0 representa el LNID del origen, si HDR.DO = 1 representa el LNID del destino.
- PKT.SPAD → 1 bit; indica si se añade relleno durante el cifrado de la carga útil.
- PKT.LEN → 9 bits; longitud de la carga útil en bytes.

2.3.3.6.2 Promotion Needed PDU

Como se ha explicado anteriormente, si un nodo está desconectado y no tiene conexión con ningún nodo *switch*, deberá enviar notificaciones a todos sus vecinos para indicar que necesita que alguno de ellos sea promocionado. Estas notificaciones se envían en forma de PNPDU. La estructura de una PNPDU se muestra a continuación:

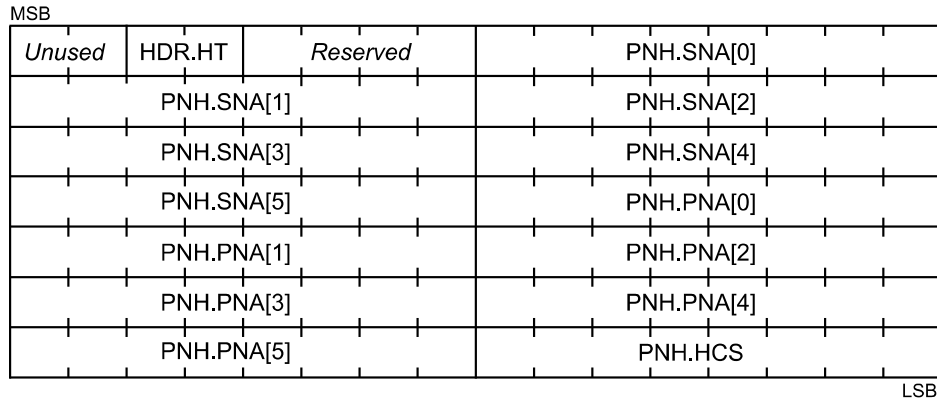


Figura 15 – Campos de la cabecera de una PNPDU [8]

- Unused → 2 bits; siempre 0.
- HDR.HT → 2 bits; tipo de cabecera (header type); HDR.HT = 1 para PNPDU
- Reserved → 4 bits; siempre 0.
- PNH.SNA → 48 bits; subnetwork address (EUI-48 del nodo base de la subred a la que se quiere conectar).
- PNH.PNA → 48 bits; promotion need address (EUI-48 del nodo transmisor).
- PNH.HCS → 8 bits; header check sequence (para detectar errores en la cabecera).

2.3.3.6.3 Beacon PDU

Todos los dispositivos *switch* en la subred transmiten una BPDU, incluido el nodo base. Su objetivo es proporcionar información de la estructura de la trama MAC y del acceso al canal al resto de dispositivos de la subred. Sus campos son los siguientes:

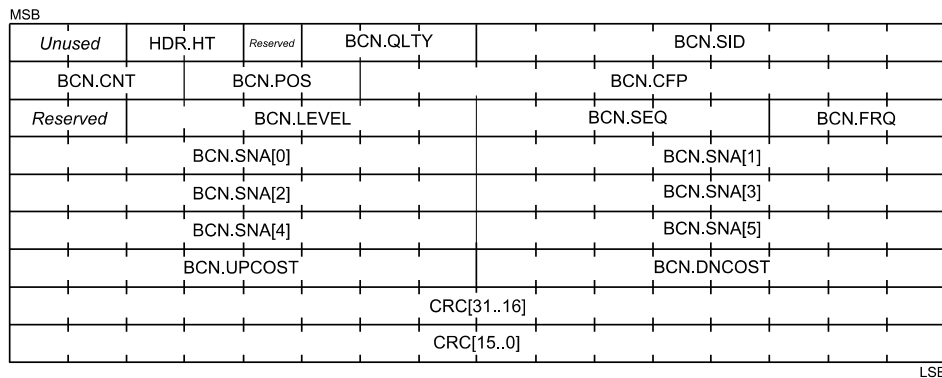


Figura 16 – Campos de una BPDU [8]

- Unused → 2 bits; siempre 0.
- HDR.HT → 2 bits; tipo de cabecera; HDR.HT = 2 para BPDU
- Reserved → 1 bit; siempre 0.
- BCN.QLTY → 3 bits; calidad de la conectividad entre este *switch* y el nodo base.
- BCN.SID → 8 bits; identificador del *switch* transmisor.
- BCN.CNT → 3 bits; número de *beacon slots* en la trama.
- BCN.SLT → 3 bits; *beacon slot* en el que se transmite esta BPDU.
- BCN.CFP → 10 bits; desplazamiento del CFP desde el principio de la trama; BCN.CFP = 0 indica que no hay CFP en la trama.
- Reserved → 1 bit; siempre 0.
- BCN.LEVEL → 6 bits; jerarquía del *switch* transmisor en la subred.
- BCN.SEQ → 5 bits; número de secuencia de esta BPDU en la supertrama.
- BCN.FRQ → 3 bits; frecuencia de transmisión de esta BPDU.
- BCN.SNA → 48 bits; identificador de la subred (EUI-48 del nodo base).
- BCN.UPCOST → 8 bits; coste total del enlace ascendente desde el *switch* transmisor hasta el nodo base.
- BCN.DNCOST → 8 bits; coste total del enlace descendente desde el nodo base hasta el *switch* transmisor.
- CRC → 32 bits

La BPDU también sirve para detectar cuando el *switch* del enlace ascendente ya no está disponible. Si un nodo de servicio deja de recibir un número mínimo de BPDUs se debe declarar este *switch* como fuera de servicio.

2.3.3.6.4 Paquetes de control MAC

Los diferentes paquetes de control de la capa MAC se muestran en la siguiente tabla:

Type (PKT.CTYPE)	Packet name	Packet description
1	REG	Registration management
2	CON	Connection management
3	PRO	Promotion management
4	BSI	Beacon slot indication
5	FRA	Frame structure change
6	CFP	Contention-free period request
7	ALV	Keep-alive
8	MUL	Multicast management
9	PRM	PHY robustness management
10	SEC	Security information

Tabla 1 – Tipos de paquetes de control [8]

▪ **Paquete de control REG (PKT.CTYPE = 1)**

Este paquete de control se utiliza para negociar el proceso de registro. El significado de este paquete difiere según su dirección. Estos paquetes son utilizados durante los procesos de registro y cancelación de registro. La siguiente tabla muestra las posibles interpretaciones de estos paquetes.

Name	HDR.DO	PKT.LNID	REG.N	REG.R	Description
REG_REQ	0	0x3FFF	0	R	Registration request <ul style="list-style-type: none"> If R=0 any previous connection from this node should be lost; If R=1 any previous connection from this node should be maintained.
REG_RSP	1	< 0x3FFF	0	R	Registration response. This packet assigns the PCK.LNID to the service node.
REG_ACK	0	< 0x3FFF	0	R	Registration acknowledged by the service node.
REG_REJ	1	0x3FFF	1	0	Registration rejected by the base node.
REG_UNR_S	0	< 0x3FFF	1	0	<ul style="list-style-type: none"> After a REG_UNR_B: unregistration acknowledge Alone: unregistration request initiated by the node
REG_UNR_B	1	< 0x3FFF	1	0	<ul style="list-style-type: none"> After a REG_UNR_S: unregistration acknowledge Alone: unregistration request initiated by the base node

Tabla 2 – Tipos de paquetes de control REG [8]

▪ **Paquete de control CON (PKT.CTYPE = 2)**

Este paquete de control se utiliza para negociar las conexiones. El significado del paquete cambia dependiendo de la dirección. Sus diferentes interpretaciones se muestran en la siguiente tabla

Name	HDR.DO	CON.N	Description
CON_REQ_S	0	0	Connection establishment request initiated by the service node.
CON_REQ_B	1	0	The base node will consider that the connection is established with the identifier CON.LCID. <ul style="list-style-type: none"> After a CON_REQ_S: connection accepted Alone: Connection establishment request
CON_CLS_S	0	1	The service node considers this connection closed: <ul style="list-style-type: none"> After a CON_REQ_B: connection rejected by the node After a CON_CLS_B: connection closing acknowledge Alone: connection closing request
CON_CLS_B	1	1	The base node will consider that the connection is no longer established. <ul style="list-style-type: none"> After a CON_REQ_S: connection establishment rejected by the base node After a CON_CLS_S: connection closing acknowledge Alone: connection closing request

Tabla 3 – Tipos de paquetes de control CON [8]

▪ **Paquete de control PRO (PKT.CTYPE = 3)**

Este paquete se utiliza para promocionar un nodo de servicio de la función terminal a la función *switch*. Al igual que con los demás paquetes de control, su

interpretación difiere dependiendo de su dirección, tal y como se muestra en la siguiente tabla.

Name	HDR.DO	PRO.N	PRO.NSID	Description
PRO_REQ_S	0	0	0xFF	Promotion request initiated by the service node.
PRO_REQ_B	1	0	< 0xFF	The base node will consider that the service node has promoted with the identifier PRO.NSID. <ul style="list-style-type: none"> After a PRO_REQ: promotion accepted Alone: promotion request initiated by the base node
PRO_ACK	0	0	< 0xFF	Promotion acknowledge
PRO_REJ	1	1	0xFF	The base node will consider that the service node is demoted. It is sent after a PRO_REQ to reject it.
PRO_DEM_S	0	1	< 0xFF	The service node considers that it is demoted: <ul style="list-style-type: none"> After a PRO_DEM_B: demotion accepted After a PRO_REQ_B: promotion rejected Alone: demotion request.
PRO_DEM_B	1	1	< 0xFF	The base node considers that the service node is demoted. <ul style="list-style-type: none"> After a PRO_DEM_S: demotion accepted Alone: demotion request

Tabla 4 – Tipos de paquetes de control PRO [8]

▪ **Paquete de control BSI (PKT.CTYPE = 4)**

El paquete de control BSI (Beacon Slot Information) solamente se utiliza por el nodo base y los nodos *switch* para intercambiar información que será utilizada por un nodo *switch* para transmitir su baliza. En el paquete BSI se incluye información acerca del número de slots y del slot que se asigna a cada *switch* para la transmisión de sus BPDUs.

Name	HDR.DO	Description
BSI_ACK	0	Acknowledgement of receipt of BSI control message
BSI_IND	1	Beacon-slot change command

Tabla 5 – Tipos de paquetes de control BSI [8]

▪ **Paquete de control FRA (PKT.CTYPE = 5)**

El paquete de control FRA es transmitido en broadcast desde el nodo base y retransmitido por todos los nodos *switch* al conjunto de la subred. Se utiliza para proporcionar información acerca del cambio de la estructura de una trama.

Name	FRA.TYP	Description
FRA_BCN_IND	0	Indicates changes to frame structure due to change in the beacon-slot count
FRA_CFP_IND	1	Indicates changes to frame structure due to change in CFP duration as a result of grant of CFP or end of CFP period for any requesting service node in the subnetwork.

Tabla 6 – Tipos de paquetes de control FRA [8]

▪ **Paquete de control CFP (PKT.CTYPE = 6)**

Este mensaje de control es utilizado para la asignación de tiempo en el acceso al canal CFP para nodos terminales o *switch*. El periodo libre de contienda no se implementa en la actualidad.

▪ **Paquete de control ALV (PKT.CTYPE = 7)**

Los mensajes de control ALV son utilizados para señalización keep-alive entre el nodo de servicio, el nodo de servicio del nivel superior y el nodo base.

Name	HDR.DO	Description
ALV_S	0	Keep-alive message from a service node
ALV_B	1	Keep-alive message from the base node

Tabla 7 – Tipos de paquetes de control ALV [8]

▪ **Paquete de control MUL (PKT.CTYPE = 8)**

El mensaje de control MUL se utiliza para controlar a los miembros de los grupos multicast.

Name	HDR.DO	MUL.N	Description
MUL_JOIN_S	0	0	Multicast group join request initiated by the service node, or an acknowledgement when sent in response to a MUL_JOIN_B.
MUL_JOIN_B	1	0	The base node will consider that the group has been joined with the identifier MUL.LCID. <ul style="list-style-type: none"> After a MUL_JOIN_S: join accepted Alone: group join request
MUL_LEAVE_S	0	1	The service node leaves the multicast group: <ul style="list-style-type: none"> After a MUL_JOIN_B: join rejected by the node After a MUL_LEAVE_B: group leave acknowledge Alone: group leave request.
MUL_LEAVE_B	1	1	The base node will consider that the service node is no longer a member of the multicast group. <ul style="list-style-type: none"> After a MUL_JOIN_S: group join rejected by the base node After a MUL_LEAVE_S: group leave acknowledge Alone: group leave request.

Tabla 8 – Tipos de paquetes de control MUL [8]

▪ **Paquete de control PRM (PKT.CTYPE = 9)**

Los paquetes PRM (PHY Robustness Management) son utilizados para controlar los parámetros que afectan a la eficiencia y robustez de la capa física.

Name	PRM.R	PRM.N	Description
PRM_REQ	0	0	PHY modulation management request
PRM_ACK	1	0	PHY modulation management acknowledge
PRM_REJ	1	1	PHY modulation management rejected

Tabla 9 – Tipos de paquetes de control PRM [8]

- **Paquete de control SEC (PKT.CTYPE = 10)**

Este tipo de mensaje es enviado como broadcast por el nodo base y todos los nodos *switch* al resto de la subred para proporcionar la secuencia aleatoria utilizada para generar claves.

2.3.3.7 Procedimientos MAC

2.3.3.7.1 Registro

Cuando se enciende un nodo de servicio en la subred, se inicia un procedimiento de registro. Un nodo de servicio en estado funcional desconectado transmitirá un paquete de control REG al nodo base para registrarse en la subred. Para que se produzca el registro, el nodo base debe asignar al nodo que quiere registrarse un LNID que ha de ser único dentro de todo el dominio del nodo switch a través del cual se conecta. Este LNID se indica en el campo PKT.LNID del mensaje de respuesta (REG_RSP) y, en combinación con el SID del nodo switch a través del cual se pretende conectar a la subred el nuevo nodo, forman el NID del nuevo nodo. Una vez recibida la respuesta, el nodo de servicio debe enviar un ACK de registro (reconocimiento de registro) al nodo base.

El paquete de control REG no está encriptado en ninguna de sus variantes. Sin embargo, sus campos REG.SNK y REG.AUK (utilizados en procesos de autenticación) sí que estarán encriptados mediante una clave inicial.

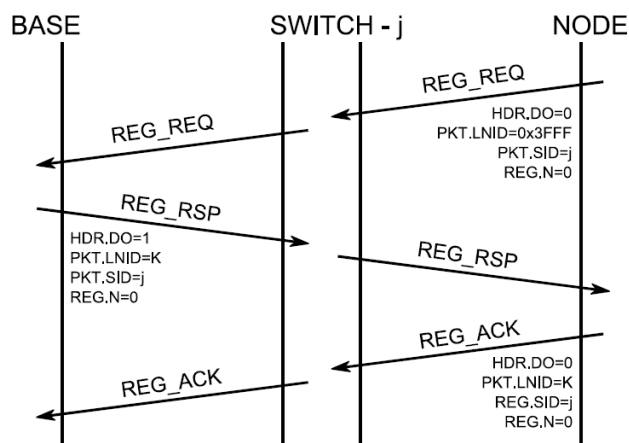


Figura 17 – Proceso de registro aceptado [8]

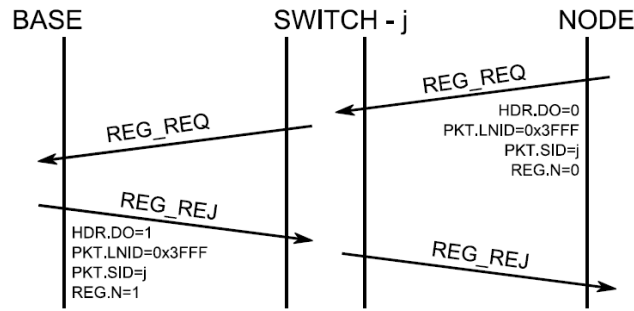


Figura 18 – Proceso de registro rechazado [8]

2.3.3.7.2 Cancelación de registro

Tanto el nodo base como cualquier nodo de servicio pueden optar por cancelar un registro existente. La secuencia de mensajes para la cancelación del registro de muestra a continuación.

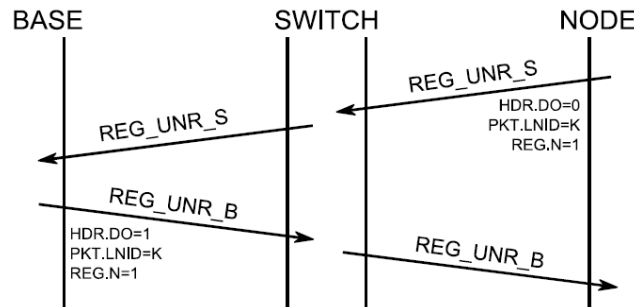


Figura 19 – Proceso de cancelación de registro iniciado por un nodo terminal [8]

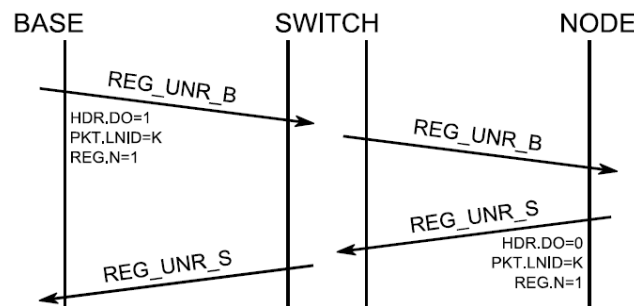


Figura 20 – Proceso de cancelación de registro iniciado por el nodo base [8]

2.3.3.7.3 Promoción

Un nodo que no esté directamente conectado a un nodo *switch* de la subred puede enviar tramas PNPDU para que un nodo terminal cercano sea promocionado y pase a ser *switch*. Durante este proceso, el nodo terminal recibirá PNPDU y generará un paquete PRO_REQ que enviará al nodo base. El nodo base examina dicha solicitud y decide si aceptarla o no. Una que decide qué nodo será el promocionado, envía un

mensaje de respuesta. El resto de nodos, los que no han sido promocionados, no recibirán ninguna respuesta a su solicitud. En situaciones especiales, el nodo base puede rechazar la promoción.

Inicialmente, cuando el nodo terminal solicita la promoción, el campo PRO.NSID en el mensaje PRO_REQ_S está fijado a todo unos. El campo PRO.NSID del mensaje de respuesta PRO_REQ_B contendrá un LSID asignado al nodo que va a ser promocionado, que lo reconocerá mediante un ACK que puede ser utilizado por nodos *switch* intermedios para actualizar sus tablas de *switching*.

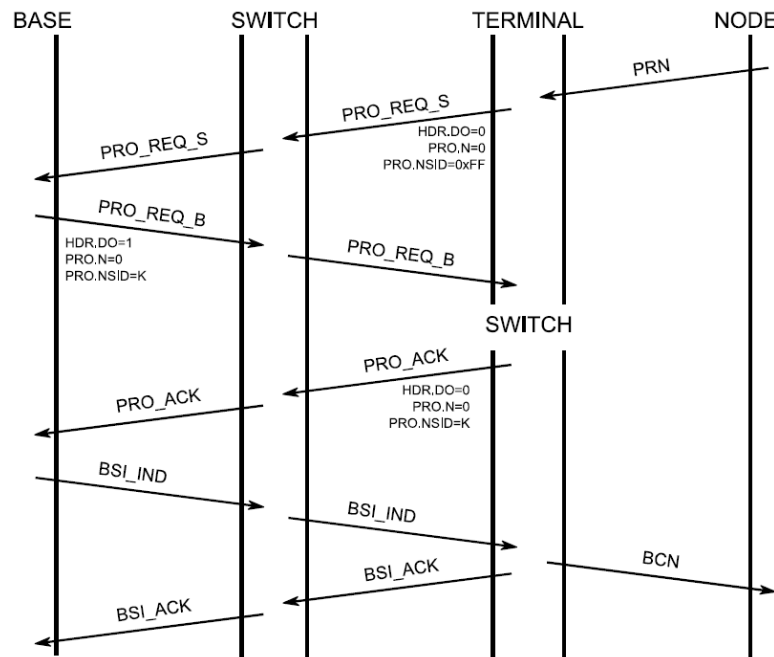


Figura 21 – Proceso de promoción iniciado por un nodo de servicio [8]

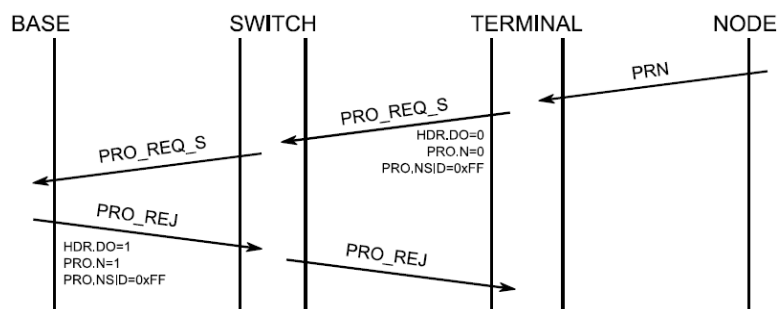


Figura 22 – Proceso de promoción rechazado por el nodo base [8]

El nodo base también puede iniciar el proceso de promoción en determinadas situaciones.

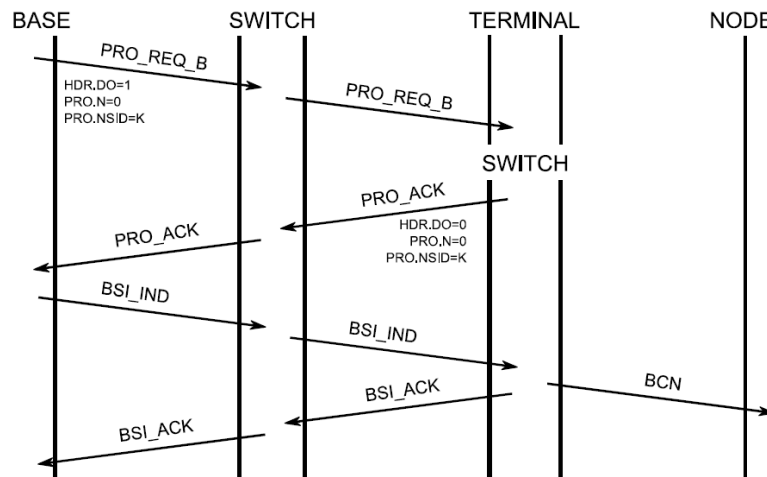


Figura 23 – Proceso de promoción iniciado por el nodo base [8]

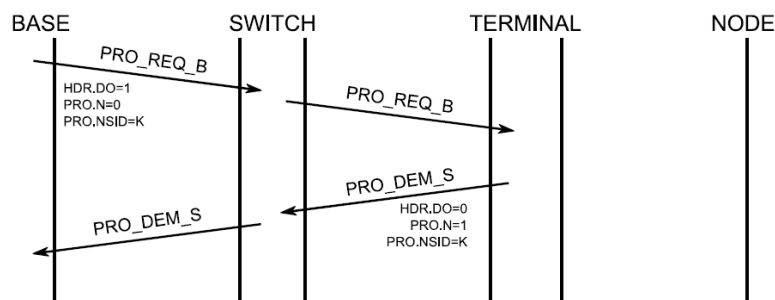


Figura 24 – Proceso de promoción rechazado por un nodo de servicio [8]

2.3.3.7.4 Proceso de degradación

El nodo base o un nodo *switch* pueden decidir la degradación de este último en cualquier momento. Para este proceso también se utiliza el paquete de control PRO. El campo PRO.NSID contiene el SID del nodo que va a ser degradado. Inmediatamente después de terminar la degradación, el nodo afectado dejará transmitir balizas y su LSID puede ser reasignado por el nodo base transcurrido un determinado tiempo.

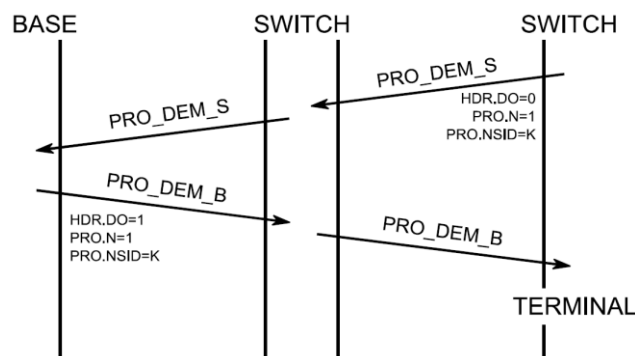


Figura 25 – Proceso de degradación iniciado por un nodo de servicio [8]

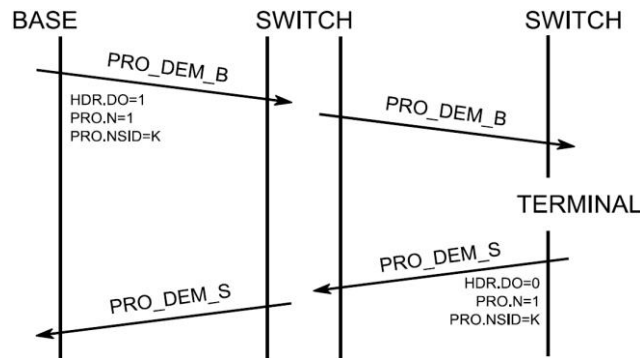


Figura 26 – Proceso de degradación iniciado por el nodo base [8]

2.3.3.7.5 Proceso de keep-alive

El proceso de keep-alive es utilizado para detectar cuando un nodo de servicio abandona la subred debido a cambios en la configuración de la red o debido a errores de los que no se puede recuperar.

Durante el registro, cuando recibe el paquete REG_RSP, el nodo de servicio utiliza el campo REG.TIME para iniciar un contador. Dicho contador se reinicia cada vez que el nodo de servicio recibe un mensaje ALV_B por parte del nodo base, utilizando el valor del campo ALV.TIME. Al recibir el mensaje ALV_B, el nodo de servicio debe enviar un mensaje ALV_S al nodo base. Si el contador expira, el nodo de servicio asume que ha sido desregistrado de la subred por el nodo base. El mensaje PRO_REQ también reinicia el valor del contador de keep-alive al valor PRO.TIME.

Cada nodo *switch* en el camino de un mensaje ALV_B debe guardar una copia del valor del contador definido en PRO.TIME y ALV.TIME, de modo que si en este tiempo no recibe ningún mensaje ALV_S de parte del nodo en cuestión, se procede al desregistro de dicho nodo por parte del nodo base.

Los posibles valores del campo ALV.TIME son los siguientes:

ALV.TIME	3 bits	<p>Time to wait for ALV_B messages before assuming the service node has been unregistered by the base node.</p> <p>ALV.TIME = 0 => 32 seconds</p> <p>ALV.TIME = 1 => 64 seconds</p> <p>ALV.TIME = 2 => 128 seconds ~ 2.1 minutes</p> <p>ALV.TIME = 3 => 256 seconds ~ 4.2 minutes</p> <p>ALV.TIME = 4 => 512 seconds ~ 8.5 minutes</p> <p>ALV.TIME = 5 => 1024 seconds ~ 17.1 minutes</p> <p>ALV.TIME = 6 => 2048 seconds ~ 34.1 minutes</p> <p>ALV.TIME = 7 => 4096 seconds ~ 68.3 minutes</p>
----------	--------	---

Tabla 10 – Posibles valores del campo ALV.TIME [8]

2.3.3.7.6 Establecimiento de conexión

El establecimiento de la conexión es un proceso extremo a extremo y conecta las capas de aplicación de los nodos que se comunican. La mayoría de las conexiones involucran al nodo base a un extremo y a un nodo de servicio en el otro. Sin embargo, puede haber caso en los que dos nodos de servicio dentro de la misma subred necesiten establecer conexión. Este tipo de conexiones se denominan conexiones directas. Las conexiones directas no se implementan en el ámbito de este TFG.

Todos los mensajes para el establecimiento de la conexión utilizan el paquete de control CON. A cada conexión el nodo base le asigna un LCID único para un LNID dado.

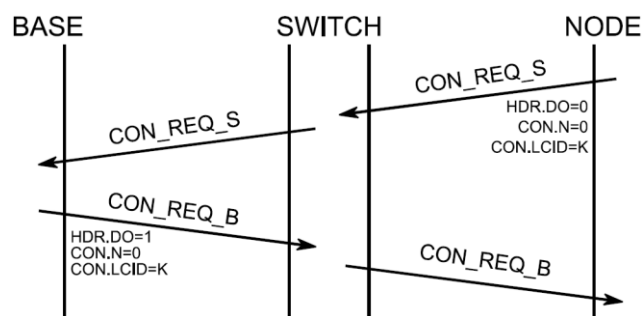


Figura 27 – Establecimiento de conexión iniciado por un nodo de servicio [8]

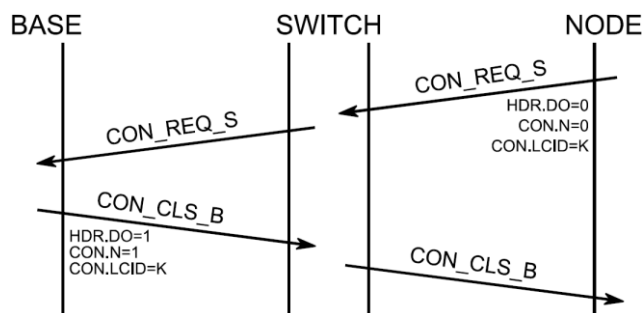


Figura 28 – Conexión rechazada por el nodo base [8]

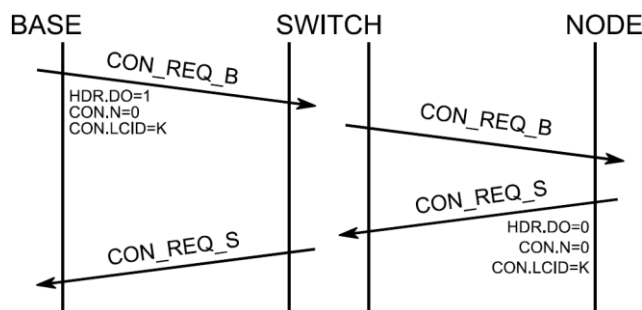


Figura 29 – Establecimiento de conexión iniciado por el nodo base [8]

2.3.3.7.7 Cierre de conexión

Cualquier dispositivo a ambos extremos de la conexión puede decidir cerrar dicha conexión en cualquier momento. Para ello, al igual que en el establecimiento de conexión, se utiliza el paquete de control CON, aunque solamente el campo CON.N es relevante a la hora de cerrar una conexión. Un cierre de conexión solicitado desde un extremo debe ser reconocido desde el otro extremo.

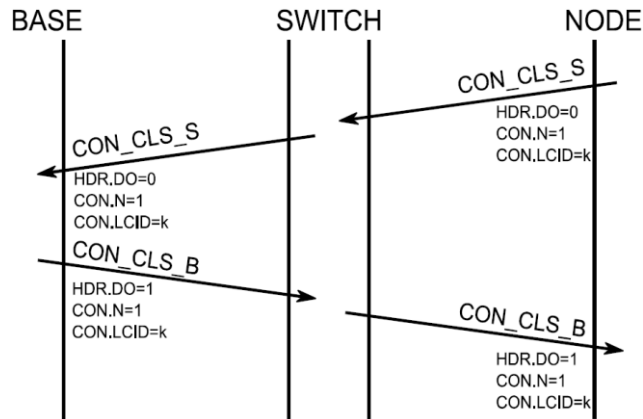


Figura 30 – Desconexión iniciada por un nodo de servicio [8]

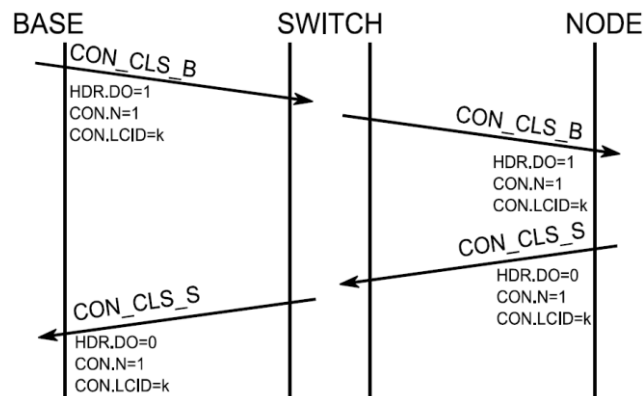


Figura 31 – Desconexión iniciada por el nodo base [8]

2.3.3.7.8 Gestión de robustez de la capa física

La capa física (PHY) tiene varios parámetros que afectan a la calidad de la transmisión como la potencia de transmisión y el esquema de modulación. El transmisor necesita feedback acerca de la calidad de recepción para ajustar sus parámetros de transmisión. Este feedback se envía utilizando paquetes de control PRM.

Existen varias fuentes de información que pueden ser utilizadas para saber si la robustez de la capa física es la adecuada o no:

- Paquetes recibidos con CRC no válido.

- Retransmisiones ARQ.
- Retransmisiones de paquetes de control.
- Solicitudes PRM enviadas por otros nodos al mismo nodo *switch*.
- Respuestas PRM.

Esta información puede ser utilizada para decidir cuándo notificar que la robustez de la capa física debe ser cambiada.

Como se ha mencionado, tanto la potencia de transmisión como la modulación afectan a la calidad de la transmisión y pueden ser ajustados dependiendo de las necesidades de la transmisión. Por lo general, se siguen las siguientes reglas:

- Aumentar la robustez: aumentar la potencia de transmisión y, si no es posible, mejorar la robustez del esquema de modulación (reduciendo el rendimiento).
- Reducir la robustez: reducir la robustez del esquema de modulación (aumentando el rendimiento) y, si no es posible, reducir la potencia de transmisión.

2.3.4 Capa de Control de Enlace Lógico (LLC)

La capa de Control de Enlace Lógico (LLC), perteneciente a la capa de Convergencia, es responsable de manejar las conexiones lógicas. Identifica cada transacción con un número de identificación y realiza los procesos de control de flujo. El control de flujo está implementado en PRIME mediante el establecimiento de una Unidad Máxima de Transmisión (MTU) y mediante la utilización de un procedimiento de ventana deslizante. La MTU define la longitud en bytes del mayor paquete de datos que puede encapsular el nivel MAC. En caso de que la aplicación intente enviar un mensaje mayor, la capa LLC fragmenta el mensaje en varios paquetes, ninguno de los cuales será mayor que la MTU. Cada uno de estos paquetes está etiquetado con un identificador para que la parte receptora pueda reensamblarlos [15].

Con respecto al procedimiento de ventana deslizante, PRIME establece diferentes valores permitidos para el Tamaño de Ventana (WS). El valor del WS puede jugar un rol importante en el rendimiento de la red en términos de latencia. Además, los dispositivos PRIME pueden implementar o no capacidades de Repetición de Solicitudes (ARQ) para asegurar la correcta recepción de todos los mensajes. Dado que los parámetros ARQ son negociados en la fase de conexión, este proceso funciona de punto a punto entre el transmisor final y el receptor, siendo por tanto los *switches* transparentes al mismo [16].

2.3.5 Capa de aplicación

En la capa de aplicación se utiliza el estándar DLMS/COSEM en PRIME en particular, pero también en el resto de tecnologías NB-PLC disponibles. El protocolo DLMS/COSEM será visto en detalle en el próximo apartado.

2.4 DLMS/COSEM

2.4.1 General

DLMS/COSEM (IEC 62056) es un protocolo de capa de aplicación específicamente diseñado para la comunicación con contadores inteligentes. COSEM es el modelo de datos y DLMS es el protocolo de capa de aplicación de PRIME que define el intercambio de los datos entre equipos de medida. DLMS/COSEM soporta múltiples protocolos de capas inferiores. Soporta comunicación sobre TCP, UDP, RS-232, RS-485 y múltiples protocolos PLC.

DLMS (*Distribution Line Message Specification*) es el protocolo utilizado en la capa de aplicación de PRIME. Es independiente de las capas inferiores y, por tanto, del canal de comunicación y está diseñado para soportar mensajes con origen o destino en dispositivos de distribución de energía en un entorno informático. Sus siglas han evolucionado hacia *Device Language Message Specification* con el objetivo de proporcionar un entorno interoperable para modelado estructurado e intercambio de datos entre contadores. Soporta funcionalidades como lectura remota de contadores, control remoto y servicios de valor añadido para medir cualquier tipo de energía, como electricidad, agua, gas o calefacción, lo que lo convierte en un factor clave en la digitalización del sector energético.

COSEM (*COmpanion Specification for Energy Metering*) es el modelo de datos. Proporciona una descripción funcional del contador en base a su interfaz. El modelado utiliza un enfoque orientado a objetos. Un objeto está formado por atributos y métodos de acuerdo a una *interface class*. Los atributos son de diferentes tipos (*data type*, *integer*, *array*, etc.) y pueden organizarse en perfiles (de carga, histórico, eventos, etc.). Para la identificación de objetos se utiliza el sistema de identificación OBIS (*OBject Identification System*).

También se define el protocolo de capa de aplicación xDLMS (*extended dlms*). Esta extensión de DLMS especifica cómo construir mensajes para acceder a los métodos y atributos de los objetos COSEM.

2.4.2 Modelo de comunicación

La especificación DLMS/COSEM está basada en el modelo OSI para modelar el intercambio de información (mensajes DLMS y datos COSEM) entre contadores y sistemas de almacenamiento de datos.

Las funciones de aplicación de los dispositivos de medida y los sistemas de almacenamiento de datos son modelados por Procesos de Aplicación (APs o

Application Processes). La comunicación entre APs es modelada por comunicación entre entidades de aplicación (AEs o *Application Entities*). Una AE representa las funciones de comunicación en un AP. En un AP puede haber varios conjuntos de funciones de comunicación OSI, de modo que un único AP puede estar representado por múltiples AEs. Sin embargo, cada AE representa a un único AP. Una AE contiene un conjunto de capacidades de comunicación llamados ASEs (*Application Service Elements*).

El intercambio de datos entre sistemas de almacenamiento de datos y dispositivos de medida está basado en el modelo cliente/servidor, donde los sistemas de almacenamiento de datos (concentrador) juegan el papel del cliente y los dispositivos de medida (contadores inteligentes) hacen de servidor. El cliente envía solicitudes de servicio (*service requests*) al servidor, que envía respuestas de servicio (*service responses*). Además, el servidor puede iniciar solicitudes de servicio para informar al cliente de eventos o para enviar datos en condiciones pre-configuradas.

En general, los APs del cliente y el servidor se encuentran en dispositivos separados, por tanto, el intercambio de mensajes tiene lugar vía pila de protocolos como se muestra a continuación.

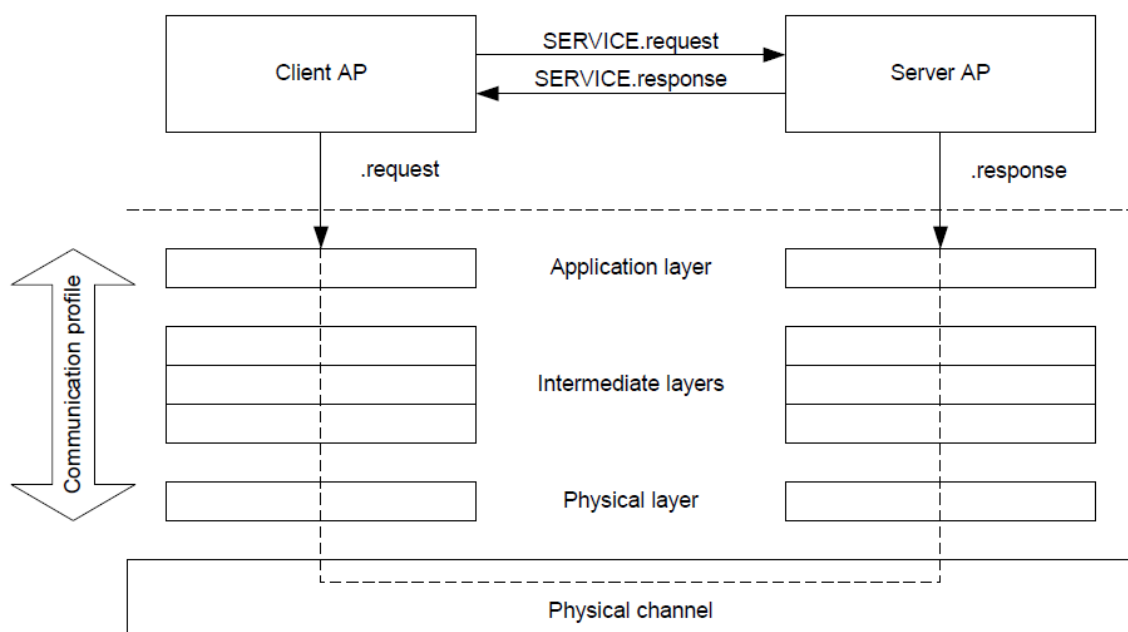


Figura 32 – Relación y protocolos cliente/servidor [17]

2.4.3 Dispositivos físicos y lógicos

En DLMS/COSEM, un contador inteligente físico (dispositivo físico) puede albergar varios de los llamados dispositivos lógicos. Cada dispositivo lógico tiene una dirección en el rango [0, 16383]. Como ejemplo, un contador puede consistir en un dispositivo lógico para la medición de electricidad con dirección 18 y otro dispositivo

lógico para un contador de gas con dirección 67. El dispositivo físico puede contener múltiples dispositivos lógicos, aunque solo se tratará el caso en el que hay un solo dispositivo lógico (el dispositivo lógico de gestión) [18].

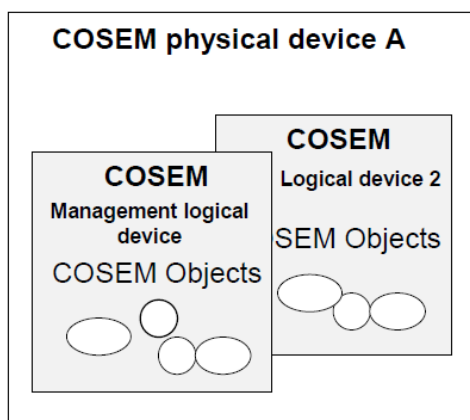


Figura 33 – Modelo de servidor COSEM [19]

2.4.3.1 Clientes

El dispositivo lógico tiene 4 asociaciones: cliente público (ID de cliente 16), cliente de lectura (ID de cliente 2), cliente de gestión (ID de cliente 1) y cliente de actualización de firmware (ID de cliente 3).

- **Cliente público**

El cliente público solo tiene utilidad para propósitos de prueba, ya que, al tener el perfil de seguridad más bajo, no tiene acceso a la lectura de datos de medida ni a realizar ningún tipo de programación en los equipos. Su papel consiste únicamente en ayudar a revelar la estructura interna del dispositivo físico.

- **Cliente de lectura**

El cliente de lectura tiene acceso a la lectura de parámetros y datos de energía. El acceso debe ser obligatoriamente por medio de contraseña.

- **Cliente de gestión**

El cliente de gestión es el utilizado por el concentrador de datos o por el servidor de acceso central para establecer tanto conexiones punto a punto como broadcast con los contadores. Este cliente puede realizar cualquier tipo de operación permitida en los dispositivos, excepto las relacionadas con la actualización de firmware. Se requiere acceso mediante contraseña.

- **Cliente de actualización de firmware**

Este cliente es el que debe ser utilizado para los procesos de actualización de firmware y, por tanto, solo está autorizado a realizar funciones de actualización de firmware. Se requiere acceso mediante contraseña.

2.4.3.2 Niveles de acceso

Para cada cliente se debe gestionar el acceso a cada uno de los atributos. Se trata de los derechos de acceso *Get*, *Set*, *Action* y *Access*.

- El servicio *Get* es utilizado por el cliente para solicitar al servidor que le devuelva el valor de uno o más atributos de objetos COSEM.
- El servicio *Set* es utilizado por el cliente para solicitar al servidor que cambie el valor de uno o más atributos de objetos COSEM.
- El servicio *Action* es utilizado por el cliente para solicitar al servidor que invoque uno o más métodos de objetos COSEM.
- El servicio *Access* es un servicio unificado que puede ser utilizado por el cliente para acceder a múltiples atributos y/o métodos con una sola solicitud.

Dependiendo del cliente, ciertos atributos pueden no ser accesibles. El cliente de lectura debe tener derechos de acceso para leer cualquier atributo, parámetro o registro de datos. El cliente de gestión debe poder gestionar todos los atributos necesarios para una correcta explotación y mantenimiento de cualquier red, incluidos derechos de acceso para leer sobre cualquier objeto y escribir sobre cualquier atributo o método, con la única excepción de los objetos relacionados con funciones de actualización de firmware. El cliente de actualización de firmware debe ser capaz de gestionar todos los objetos, atributos y métodos relacionados con funciones de actualización de firmware.

Para acceder a los atributos y métodos de objetos COSEM, estos tienen que ser referenciados. Existen dos métodos de referenciación:

- Referenciación LN (*Logical Name Referencing*). Los atributos y métodos son referenciados mediante el “nombre lógico” (código OBIS) de la instancia del objeto COSEM al que pertenecen. Es un número de 6 bytes que identifica de manera única un objeto dentro de un dispositivo lógico. Por ejemplo, el reloj de un contador inteligente es alcanzable siempre bajo la dirección [0, 0, 1, 0, 0, 255]. En el contexto LN, los servicios relevantes son *Get* (lectura) y *Set* (escritura), *Action* y *Access*.
- Referenciación SN (*Short Name Referencing*). Los nombres cortos son utilizados para dispositivos pequeños, y solo deben ser usados cuando el contador inteligente conectado a estos no puede comunicarse utilizando nombres

lógicos. Cuando se utiliza este tipo de referenciación, el contador todavía conserva un nombre lógico único para cada uno de sus objetos. Además, cada objeto tiene un nombre corto de 2 bytes que se asigna al nombre lógico. Por tanto, un cliente puede direccionar cada atributo o método utilizando solamente 2 bytes.

El cliente siempre utilizará referenciación LN, mientras que el servidor podrá utilizar tanto referenciación LN como SN.

2.4.4 Funcionamiento orientado a conexión

Una sesión de comunicación consta de tres fases, como se puede ver en la siguiente figura:

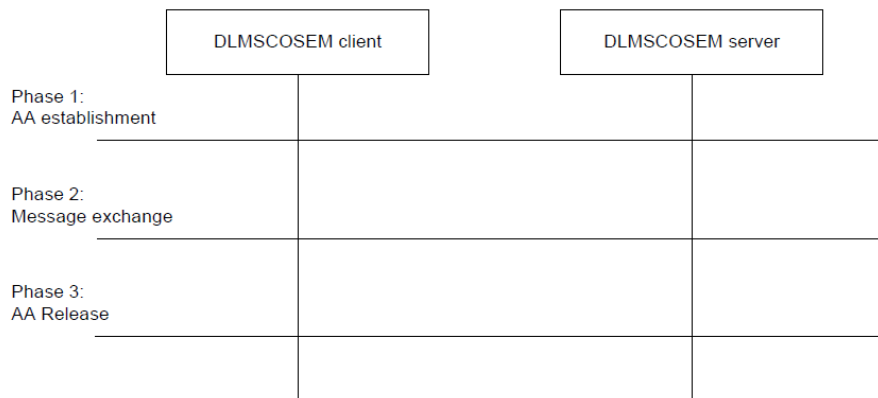


Figura 34 – Sesión de comunicación completa en el entorno orientado a conexión [20]

- En primer lugar, se establece una conexión a nivel de aplicación, llamada Asociación de Aplicación (AA o *Application Association*) entre el cliente y el servidor.
- Una vez que la AA se ha establecido, puede comenzar el intercambio de mensajes.
- Cuando el intercambio de información ha concluido, la AA se libera.

2.4.5 Asociaciones de aplicaciones (AAs)

Las asociaciones de aplicaciones (AAs) son conexiones lógicas entre un cliente y un servidor. Las AAs pueden ser establecidas en la solicitud de un cliente o puede ser Pre-establecida. También pueden ser confirmadas o no confirmadas.

Un dispositivo lógico COSEM puede soportar una o más asociaciones, cada una con un cliente diferente. Existen dos tipos de asociaciones: confirmadas y no confirmadas. Una asociación confirmada es aquella que es propuesta por el cliente y aceptada por el servidor. Una asociación no confirmada también es propuesta por el

cliente asumiendo que el servidor la aceptará. No tiene lugar ningún tipo de negociación. Las asociaciones no confirmadas son útiles para enviar mensajes broadcast del cliente a los servidores.

2.4.5.1 Establecimiento y liberación de asociaciones

Los servicios utilizados para el establecimiento y liberación de asociaciones son: COSEM-OPEN, COSEM-RELEASE y COSEM-ABORT.

2.4.5.1.1 Establecimiento de una asociación

El servicio COSEM-OPEN se utiliza para el establecimiento de asociaciones. Las APDUs (Application Protocol Data Units) AARQ y AARE son las encargadas de transportar las primitivas del servicio COSEM-OPEN. La secuencia para el establecimiento de una asociación es la siguiente:

- Inicialmente, como resultado de invocar el servicio COSEM-OPEN.request, la capa de aplicación del cliente envía una AARQ (*Application Association ReQuest*) a la capa de aplicación del servidor. Esta solicitud contiene los parámetros que definen a la asociación.
- La capa de aplicación del servidor, como resultado de invocar el servicio COSEM-Open.response, responde a esta solicitud con una AARE a la capa de aplicación del cliente. La AARE contiene los parámetros negociados de la asociación.

Como consecuencia de las primitivas de servicio asociadas a las AARQ y AARE (COSEM-OPEN.request y COSEM-OPEN.response), en la capa de aplicación de servidor y cliente se genera las primitivas COSEM-OPEN.indication y COSEM-OPEN.confirm, respectivamente.

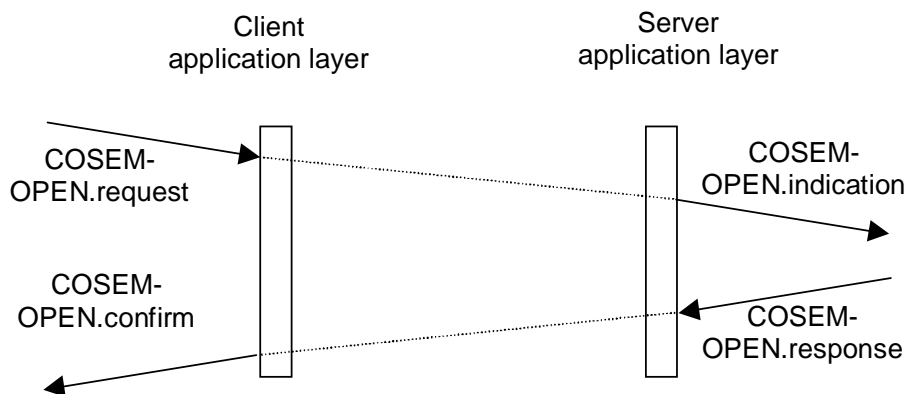


Figura 35 – Secuencia para el servicio COSEM-OPEN [21]

2.4.5.1.2 Liberación de una asociación

El servicio COSEM-RELEASE se proporciona para la desconexión voluntaria de una asociación existente. Como los procesos de aplicación del servidor no están habilitados para solicitar una desconexión voluntaria, el servicio COSEM-RELEASE.request está disponible únicamente para el cliente. La secuencia para el servicio COSEM-RELEASE es la misma que para el servicio COSEM-OPEN, pero cambiando la palabra OPEN por la palabra RELEASE.

2.4.6 Sistema de Identificación de Objetos (OBIS)

El Sistema de Identificación de Objetos (OBIS) define los códigos de identificación para los datos utilizados comúnmente en los equipos de medida. El OBIS proporciona un identificador único para todos los datos dentro del equipo de medida, incluyendo no solo valores de medidas, sino también valores abstractos utilizados para configuración o para obtener información acerca del comportamiento del equipo de medida. Estos códigos se utilizan para la identificación de:

- Nombres lógicos.
- Datos transmitidos a través de las líneas de comunicación.
- Datos mostrados en los equipos de medida.

Los códigos OBIS son una combinación de 6 bytes (o grupos de valores) que describen de manera jerárquica el significado exacto de cada elemento de datos.

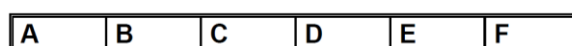


Figura 36 - Estructura del código OBIS [19]

- El grupo A define la característica del elemento de datos que queremos identificar (electricidad, gas, agua, etc.)
- El grupo B define el número del canal, es decir, el número de la entrada de un dispositivo de medición que tiene varias entradas para la medida de energía del mismo o de diferentes tipos.
- El grupo C define los elementos de datos abstractos o físicos relacionados con la fuente de información en cuestión, por ejemplo, corriente, voltaje, potencia, volumen o temperatura. La medida, procesamiento de tarifas y métodos de almacenamiento de datos de estas cantidades se definen en los grupos D, E y F.
- El grupo D define el tipo de información que queremos obtener de los elementos identificados en los grupos A y C, por ejemplo, tarificación diaria, máximo, mínimo, media actual, etc.

- El grupo E define el procesamiento adicional de los resultados de medidas anteriores para establecer registros de tarifas.
- El grupo F define el almacenamiento de datos identificados por los grupos anteriores, de acuerdo a los diferentes periodos de facturación. En la mayoría de los casos este grupo no se utiliza y está fijado a 255.

Cuando cualquiera de los valores de C a F toma un valor entre 128 y 254, el código es considerado como código específico del fabricante.

2.4.7 Perfiles de comunicación

Los perfiles de comunicación especifican cómo la capa de aplicación de DLMS/COSEM y el modelo de datos COSEM que modela los procesos de aplicación (APs) son soportados por las capas inferiores.

Los perfiles de comunicación comprenden varias capas de protocolo. Cada capa tiene una tarea distinta, proporciona servicios a su capa superior y utiliza recursos de su capa (o capas) inferiores. Los Procesos de Aplicación (AP) del cliente y del servidor utilizan los servicios de la capa de protocolo más alta, la capa de aplicación. Esta es la única capa que contiene elementos específicos COSEM: los ASE (Application Service Elements) xDLMS. El número y tipo de capas inferiores depende del medio de comunicación utilizado.

Un determinado conjunto de capas de protocolo, con la capa de aplicación DLMS/COSEM y el modelo de objetos COSEM en la parte superior constituye un perfil de comunicación DLMS/COSEM particular. Cada perfil se caracteriza por las capas de protocolo incluidas y sus parámetros.

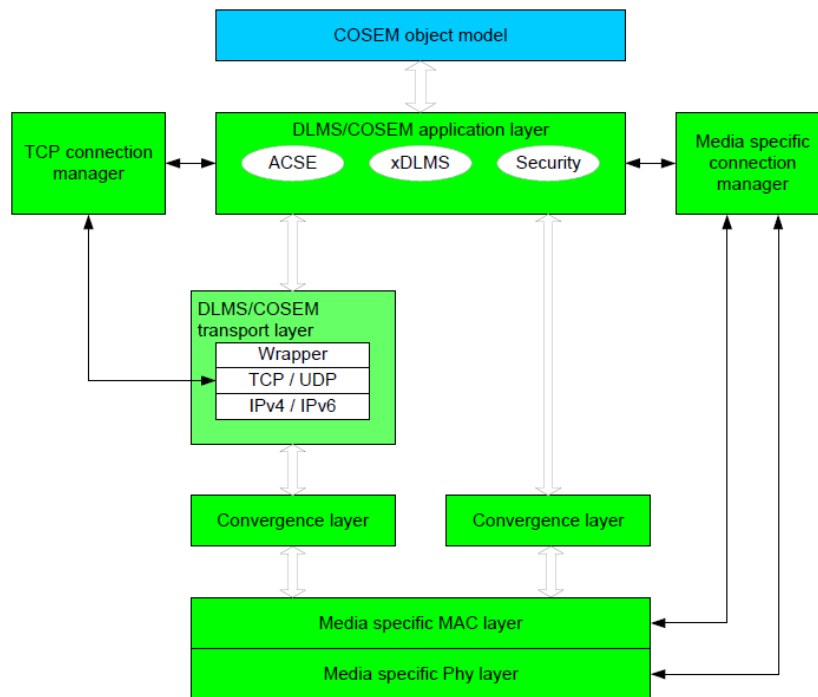


Figura 37 – Perfil de comunicación DLMS/COSEM genérico [20]

La figura anterior muestra un perfil de comunicación DLMS/COSEM genérico e incluye:

- El modelo de objetos COSEM que modela los Procesos de Aplicación.
- La capa de aplicación DLMS/COSEM.
- La capa de transporte DLMS/COSEM.
- Las capas de convergencia que unen la capa MAC con la capa de aplicación DLMS/COSEM, ya sea directamente o a través de la capa de transporte DLMS/COSEM.
- La capa física y la capa MAC del medio específico.
- Los gestores de conexión.

En el caso de este TFG, el medio específico será PRIME.

Un solo dispositivo físico puede soportar más de un perfil de comunicación. En estos casos, el AP de cliente debe decidir qué perfil de comunicación se debe utilizar.

2.5 STG-DC

STG-DC es un protocolo desarrollado por Iberdrola para cumplir los requisitos de la legislación española con respecto al despliegue de contadores inteligentes. Las versiones de este protocolo están a disposición de los miembros de la Prime Alliance. STG-DC es un protocolo de servicios web basado en SOAP y FTP, y define la comunicación bidireccional entre el Sistema de Telegestión (STG) y el Concentrador de Datos (DC o Data concentrator) [22].

Como se ha mencionado, STG-DC es un protocolo de servicios web basado en SOAP y FTP. SOAP (*Simple Object Access Protocol*) es un protocolo estándar para el intercambio de información estructurada en la implementación de servicios web en redes informáticas. SOAP permite la comunicación entre procesos en diferentes sistemas operativos utilizando XML y puede trabajar sobre cualquier protocolo de capa de aplicación capaz de transmitir texto (como HTTP, FTP o SMTP). Además, presenta la ventaja de que, debido al uso de XML, presenta una gran interoperabilidad ya que puede ser implementado utilizando cualquier lenguaje y en cualquier plataforma.

El objetivo es que el concentrador de medidas pueda ser gestionado totalmente a través del sistema de telegestión. Para ello contamos con la posibilidad de solicitar informes, bien por parte del concentrador a un contador o grupo de contadores, o bien desde el propio sistema de telegestión al concentrador. Estos informes son los Sxx y Bxx. Cuando una de estas acciones se realiza por iniciativa del concentrador se denomina modo *Push*, y cuando se trata de una solicitud del STG hablamos de modo *Pull*.

Los diferentes tipos de informes y órdenes STG-DC se pueden encontrar en el **Anexo I** de este Trabajo de Fin de Grado.

2.6 Meter Data Management Systems (MDMS)

2.6.1 General

Los MDMS (*Meter Data Management Systems*) son componentes de las infraestructuras de medición avanzadas responsables de la gestión, tratamiento y provisión de datos y difusión de los datos de consumo medidos. También pueden contener un subconjunto de información del activo del contador, topología o información del cliente. Aunque su implementación puede variar, todos los MDMS deben estar capacitados para llevar a cabo las siguientes funciones [23]:

- Almacenar datos proporcionados por el concentrador de datos.
- Gestionar comandos, como por ejemplo desconexión y conexión remota.
- Validar, editar y estimar lecturas de contadores.
- Gestionar excepciones
- Gestionar eventos, como puede ser el evento de fraude o la notificación de apagado de contadores.
- Estimar medidas no válidas.
- Calcular datos de facturación.
- Agregar medidas de contadores.
- Realizar un seguimiento del inventario de contadores.
- Proporcionar datos a aplicaciones externas, como las aplicaciones de cliente.
- Proporcionar información directamente a los usuarios finales (personal y clientes).
- Soportar funciones adicionales, como análisis de protección de beneficios, asistencia en la planificación de distribución o pago por adelantado.

Los MDMS resultan de interés para todos los subsectores incluidos en la industria energética ya que estos les permiten gestionar de manera más eficiente los datos de consumo de su infraestructura, y además mejoran la calidad de la información que el cliente recibe.

Existen numerosas empresas, algunas de ellas de gran importancia mundial, que han desarrollado y ofrecen sistemas de telegestión de contadores inteligentes para su

uso por parte de las distribuidoras. Algunas de las más importantes son Siemens, Oracle, Itron y Landis+Gyr.

- Siemens. Gran proveedor global de tecnología y soluciones para el sector de servicios públicos. Su producto MDM es EnergyIP, utilizado por 50 empresas de servicios públicos (con 55 millones de contadores bajo contrato y 20 millones de contadores operativos), según el informe Gartner para los productos MDM del año 2015 [23].
- Oracle Utilities. Oracle es un gran proveedor IT a escala mundial que ofrece un producto MDM a través de Oracle Utilities, su organización orientada a la industria de los servicios públicos. Oracle Utilities MDM está en producción en más de 40 compañías de servicios públicos con más de 35 millones de contadores [23].
- Itron. Compañía estadounidense de tecnología que ofrece un amplio rango de productos de medida y almacenamiento de datos. Su plataforma de telegestión Saturne, integrada en el sistema MDM de Itron, IEE (Itron Enterprise Edition), líder mundial en el mercado de MDMS. Existen 72 compañías que utilizan IEE MDM, con más de 37 millones de contadores [23].
- Landis+Gyr. Propiedad de Toshiba, es uno de los mayores proveedores de soluciones de medida y gestión de energía a nivel global. Su producto MDM es Gridstream MDMS y es utilizado por 25 compañías, con 23.5 millones de contadores en todo el mundo [23].

En el marco del proyecto OSIRIS, la plataforma de telegestión proporcionada para la realización de este Trabajo de Fin de Grado es IRIS, de la empresa española STM Telecontrol.

2.6.2 Plataforma de Telegestión IRIS

IRIS es la Plataforma de Telegestión abierta desarrollada por Telecontrol STM que permite explotar el potencial de las nuevas *Smart Grids* basadas en la tecnología PRIME. IRIS es un sistema para la gestión de los procesos de telegestión y telemedida, que permite gestionar dispositivos PRIME en un entorno escalable y flexible. Está basada en los IRIS Core Services, un conjunto de servicios de alto nivel abiertos, distribuidos y escalables que permiten particularizar el sistema para cualquier necesidad del cliente [24].

Una de las mayores ventajas que tienen los contadores inteligentes con respecto a los tradicionales es la de la posibilidad de realizar su gestión y mantenimiento de manera remota, sin la necesidad de que un técnico acuda de forma física al lugar de la ubicación del contador. Desde el punto de vista del consumidor, podrá beneficiarse de

una atención más rápida y disponibilidad de más información sobre la energía consumida.

IRIS implementa la siguiente funcionalidad de telemedida [25]:

- Recogida de datos diarios y mensuales.
- Gestión completa de los datos de medida.
- Tratamiento y visualización.
- Funciones de generación de gráficos de los datos recogidos.
- Informes.
- Gestionar cualquier dispositivo conectado al sistema.
- Desconexión/reconexión remota de contadores con doble mecanismo de seguridad.
- Recogida automática de contadores descubiertos por el concentrador.
- Valores Instantáneos
- Gestión de cortes de suministro.
- Gestión de incidencias de suministro.
- Configuración remota de la potencia máxima.
- Gestión de los dispositivos.
- Adición de nuevos concentradores al sistema de manera manual o automática (mediante un flujo de integración con la compañía eléctrica).
- Adición manual de contadores
- Gestión de colecciones de concentradores y contadores.
- Enviar órdenes a los concentradores y contadores.
- Geolocalización de concentradores y contadores.
- Posibilidad de crear atributos libres para los dispositivos. (por ejemplo, identificadores particulares de la compañía eléctrica, atributos de geolocalización, identificadores de clientes, etc.).

El manual de usuario de IRIS se incluye en el **Anexo II** de este Trabajo de Fin de Grado.

2.7 Infraestructura ciber-física

La infraestructura ciber-física de la que se dispone en el grupo de investigación del Departamento de Ingeniería Telemática, como se ha mencionado, consta de una parte física y otra virtual.

El segmento físico de la infraestructura está formado por 4 *Smart Meters* o contadores inteligentes (con números de serie ZIV0042540112, ZIV0042540113, ZIV0042540114 y ZIV0042540115), asociados a un concentrador de datos (con número de serie ZIV004372798). Todos los dispositivos de la infraestructura física son del fabricante ZIV. Para la captura de tráfico entre los contadores y el concentrador de la infraestructura física contamos con el *sniffer* ZIV PRIME Manager, proporcionado por el propio fabricante. Para capturar el tráfico entre el concentrador y aplicaciones de la red (interfaz web del concentrador y plataforma de telegestión) disponemos del analizador de protocolos Wireshark, de uso abierto y gratuito. La infraestructura física es gestionable en su totalidad tanto a través de la interfaz web del concentrador ZIV como de la Plataforma de Telegestión IRIS.

El esquema de la parte física de la infraestructura y del MDMS (*Meter Data Management System*), que representa la arquitectura de comunicaciones típica para Sistemas de Medición avanzada, así como los protocolos utilizados en cada sección se muestra en la siguiente figura:

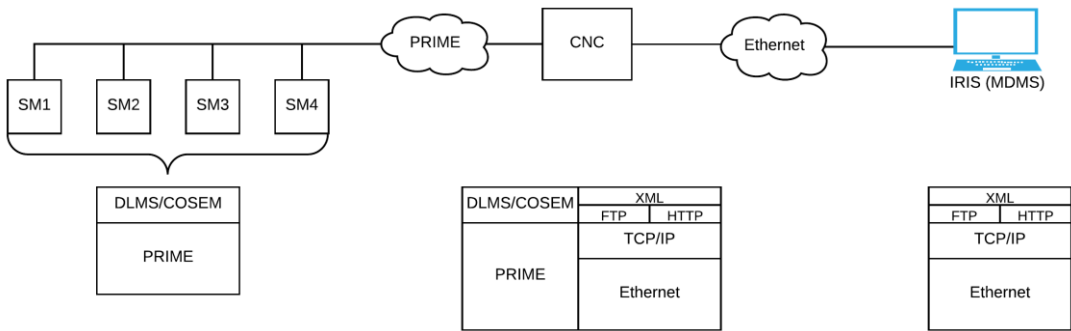


Figura 38 – Esquema de la infraestructura física

El segmento virtual de la infraestructura solamente es accesible y gestionable a través de IRIS y consta de una red mucho más amplia de concentradores y contadores con el objetivo de simular una red real administrada por una distribuidora. Concretamente, esta infraestructura virtual está formada por 10 concentradores y 1593 contadores asociados, variando el número de contadores que cada concentrador tiene asociado entre 150 y 170.

A través de IRIS podremos gestionar la infraestructura ciber-física completa, sin distinción entre la parte física y la virtual.

El esquema de la infraestructura ciber-física completa es el siguiente:

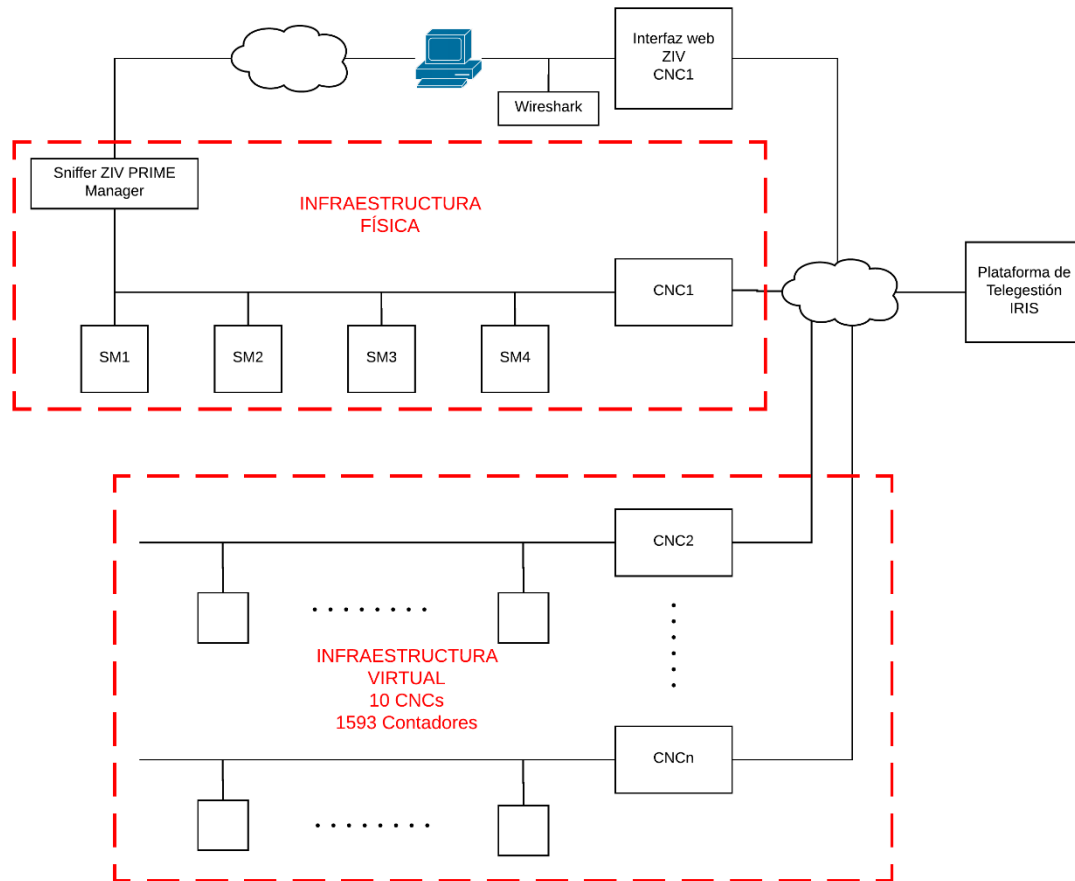


Figura 39 – Esquema de la infraestructura ciber-física

2.8 Herramientas utilizadas

2.8.1 ZIV PRIME Manager

ZIV PRIME Manager es una herramienta para la gestión y supervisión de redes PLC de baja tensión. Se trata de un *sniffer* que nos va a permitir capturar y visualizar información relacionada con el medio físico como el espectro frecuencial, tramas MAC y topología de la red PLC.

El manual de usuario de la herramienta ZIV PRIME Manager se incluye en el **Anexo III** de este TFG.

2.8.2 Interfaz Web del Concentrador ZIV

La interfaz web del concentrador ZIV nos va a permitir configurar el concentrador y establecer comunicación entre éste y los contadores en tiempo real. Desde aquí podemos solicitar diferentes informes y estadísticas al propio concentrador o a cualquiera de sus contadores asociados.

El manual de usuario de la Interfaz Web del Concentrador ZIV se incluye en el **Anexo IV** de este TFG.

2.8.3 XML Translator

XML Translator es una sencilla herramienta que permite decodificar los mensajes DLMS/COSEM en formato XML para su correcta identificación y visualización de los diferentes campos que lo componen. Descargable gratuitamente [26].

2.8.4 Obis Helper

OBIS Helper es una herramienta para decodificar códigos OBIS en su descripción de texto y también a la inversa (codificar descripción de texto en código OBIS). De este modo podemos identificar en las secuencias hexadecimales el tipo de información concreta contenida en ellas. Descargable gratuitamente [27].

2.9 Marco regulatorio

La legislación nacional y europea juega un papel crucial en el desarrollo y despliegue de las *Smart Grids*. Debido a las carencias de los sistemas convencionales de medida y a las necesidades por ello surgidas se hace necesario un marco regulatorio claro y transparente que contemple la utilización de los sistemas de medida inteligentes, a la vez que fomenta su despliegue y utilización como camino hacia las redes del futuro.

2.9.1 Marco regulatorio europeo

A nivel europeo, actualmente existen una serie de Directivas sobre mercado interior, medio ambiente, tecnologías y fiscalidad que persiguen la consecución de una política energética común, fomentando el desarrollo de los sistemas de telegestión. Asimismo, se han publicado mandatos encaminados a la implantación de contadores inteligentes y sistemas de telegestión. Las medidas legislativas relevantes para el desarrollo de las *Smart Grids* son las siguientes:

- Directiva 2004/22/CE [28], en la que se realiza una aproximación para la normalización y armonización de instrumentos de medida.
- Mandato M/374 [29], en el que la Comisión Europea solicita a los organismos CEN y CENELEC, la elaboración de los estándares necesarios para la ejecución de la Directiva 2004/22/EC.
- Directiva 2006/32/CE [30], que tiene como finalidad establecer mecanismos para eliminar los obstáculos del mercado que impidan un uso eficiente de la energía y promover las condiciones para el desarrollo de las mejoras en eficiencia energética.
- Directiva 2009/72/CE [4], la más relevante en el momento de su publicación y que trata sobre temas comunes para el mercado interior de la electricidad, como herramientas para fomentar la eficiencia energética, alcanzar precios competitivos, aumentar la calidad del servicio y la competitividad y contribuir a la seguridad del suministro y a la sostenibilidad [31].
- Directiva 2012/27/UE [32], que aborda la eficiencia energética y deroga la Directiva 2006/32/CE. Respecto a las medidas de mejora de la eficiencia energética, esta directiva destaca la importancia de la aplicación de innovaciones tecnológicas, como los contadores inteligentes, como camino a la mejora de eficiencia y ahorro.

- Recomendación 2012/148/UE [33], que comprende las recomendaciones relativas a los preparativos para el despliegue de los sistemas de contador inteligente [31].

2.9.2 Marco regulatorio español

En España, la implantación progresiva de este tipo de contadores está prevista desde el año 2007. En este año se aprobó el Real Decreto 1110/2007, por el que se aprueba el llamado “Reglamento unificado de puntos de medida del sistema eléctrico”. Posteriormente se aprueban una serie de órdenes destinadas al cumplimiento de lo establecido en el Real Decreto 1110/2007. Estas órdenes son la Orden ITC/3022/2007 [34], Orden ITC/3860/2007 [6] y Orden IET/290/2012 [35].

- Real Decreto 1110/2007, en el que se definen las bases del “Reglamento unificado de puntos de medida del sistema eléctrico”, con el que se persigue cumplir con los requisitos en lo referente a la libertad de mercado y liquidación de la energía, y también que la estructura de precios de la energía se referencie a los costes reales de suministro. Además, en este documento se establece por primera vez que los sistemas de medición no se sirven únicamente de contadores, estableciéndose las funcionalidades de los sistemas de telegestión [31].
- Orden ITC/3022/2007, que regula el control metrológico del Estado sobre los contadores inteligentes para suministros de potencia contratada inferior a 15 kW y comprende las principales funcionalidades y requisitos técnicos de dichos contadores.
- Orden ITC/3860/2007, la primera en recoger en detalle el “Plan de sustitución de equipos de medida” y que establece como fecha límite para la total sustitución de contadores tradicionales por contadores inteligentes el 31 de diciembre de 2018.
- Orden IET/290/2012, que modifica los plazos para ciertos hitos intermedios recogidos en la Orden ITC/3860/2007, pero mantiene la fecha límite en el 31 de diciembre de 2018.

Capítulo 3

Diseño de la solución

En este capítulo se describen los requisitos y restricciones para la elaboración del manual de prácticas que sirve de base para este Trabajo de Fin de Grado. Tras haber definido estos puntos, se presenta el diseño de dicho manual, en el que se plantea la batería de pruebas a realizar sobre la infraestructura ciber-física. Estas pruebas están planteadas de modo que se haga uso de las herramientas descritas en el Capítulo 2 y se ponga a prueba el conocimiento acerca de las tecnologías implicadas con el objetivo final de ilustrar el potencial de la infraestructura ciber-física y la Plataforma de Telegestión IRIS.

3.1 Requisitos y restricciones

Los requisitos y restricciones a la hora de afrontar este Trabajo de Fin de Grado vienen definidos por el proyecto OSIRIS, de ámbito nacional y promovido por Unión Fenosa Distribución, en el que se desarrolla el mismo. Todos los recursos (infraestructura, plataforma de telegestión y herramientas) utilizados en el transcurso de este TFG han sido proporcionados en el marco de este proyecto.

Para la realización de este TFG resulta necesario contar con una infraestructura de red PRIME que se asemeje a las infraestructuras reales que las distribuidoras tienen que gestionar y mantener. Para ello se cuenta con la infraestructura ciber-física detallada en el **Apartado 2.7**. En esta infraestructura se dispone de una parte física que, por cuestiones obvias de espacio, resulta limitada, de modo que su principal finalidad es la de comprender y visualizar la comunicación entre el concentrador y contadores PRIME. Esta parte física de la infraestructura está formada por equipos del fabricante ZIV, aunque esto no supone una limitación, ya que el estándar PRIME garantiza interoperabilidad entre equipos de diferentes marcas.

Resulta imprescindible también disponer de un *sniffer* para capturar tráfico entre el concentrador y los contadores PRIME de la parte física de la infraestructura. Mediante estas capturas podemos analizar la comunicación entre dispositivos PRIME, e identificar los parámetros de esta comunicación definidos en el estándar. El *sniffer* utilizado es ZIV PRIME Manager, y ha sido proporcionado por ZIV, el fabricante de los equipos físicos.

Los mensajes PRIME transportan a su vez mensajes DLMS/COSEM (protocolo de capa de aplicación de PRIME). Para traducir o decodificar estos mensajes desde hexadecimal a formato XML, de modo que se puedan visualizar tanto el tipo de mensaje como sus diferentes atributos, necesitamos utilizar la herramienta XML Translator. También dentro del ámbito de los mensajes DLMS/COSEM, es necesario decodificar el código OBIS presente en ciertos mensajes para la identificación de datos utilizados comúnmente en los equipos de medida, para lo que se dispone de la herramienta OBIS Helper. Tanto XML Translator [26] como OBIS Helper [27] son herramientas que pueden ser descargadas de manera gratuita.

Por último, un requisito indispensable, ya que buena parte de este TFG gira en torno a ello, es disponer de una plataforma para la telegestión de contadores inteligentes. La plataforma de telegestión proporcionada en el marco del proyecto OSIRIS es IRIS, desarrollada por la empresa española Telecontrol STM.

3.2 Manual de practicas

3.2.1 Introducción

En este apartado se presenta el enunciado del manual de prácticas en el que se define la batería de pruebas a realizar sobre la infraestructura ciber-física, con el fin de analizar su potencial. Este manual está enfocado a un uso académico, por lo que pretende ser lo más completo posible con el fin de ahondar en cada una de las tecnologías y herramientas que intervienen en esta infraestructura y de esta forma asegurar su correcto aprendizaje.

Para la elaboración de este manual de prácticas se han definido dos tipos de pruebas. Por un lado, se definen pruebas que permitan analizar y visualizar el funcionamiento y las funcionalidades de los protocolos de comunicaciones presentes, los cuales están explicados en anteriores apartados y, de cara a una hipotética asignatura, serían explicados en las clases teóricas. Por otro lado, se definen otras pruebas enfocadas a ilustrar la funcionalidad de la plataforma MDMS IRIS.

3.2.2 Escenario de prueba

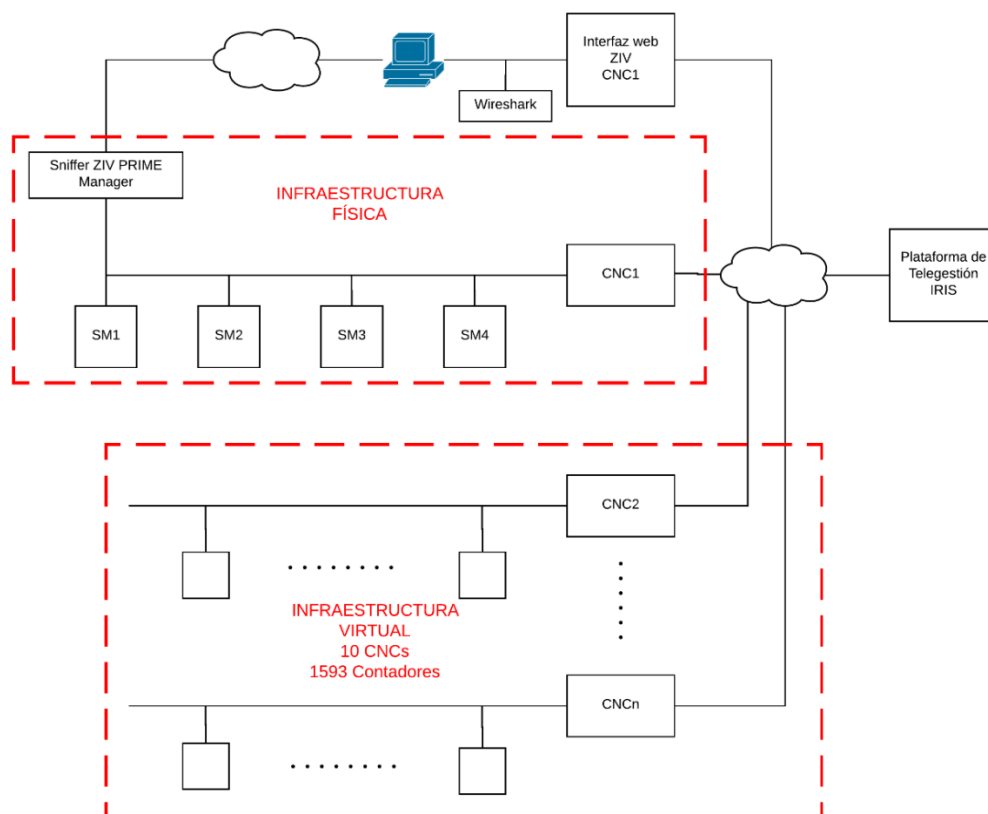


Figura 40 – Escenario de prueba (explicado en detalle en el Apartado 2.7)

3.2.3 Pruebas

A continuación, se adjuntan las pruebas a realizar sobre la infraestructura ciberfísica para telegestión de contadores inteligentes, con el objetivo de analizar el funcionamiento y potencial de dicha infraestructura. La batería de pruebas está dividida en tres bloques.

3.2.3.1 Bloque 1: Protocolo PRIME y ZIV PRIME Manager

En primer lugar, nos centraremos en el análisis de mecanismos básicos del protocolo PRIME. Para ello, nos centraremos en la infraestructura física (panel) y utilizaremos el analizador de trazas PRIME ZIV PRIME Manager para capturar tráfico durante las pruebas que se indican a continuación.

1. Con todos los contadores apagados. ¿Qué tipos de paquetes PRIME se observan? ¿Para qué sirve cada uno de ellos? ¿Hay alguno que llame especialmente la atención? En caso de que sea así, ¿a qué cree que se debe?
2. Ahora encendemos uno de los contadores. ¿Qué tipos de paquetes PRIME se observan? ¿Para qué sirve cada uno de ellos? ¿En qué mensaje asigna el concentrador el NID (SID + LNID) al contador?
3. Apagamos ahora el contador. ¿Qué mecanismo tiene el concentrador para detectar si un contador está encendido o apagado? ¿Cómo (o cuándo) se da cuenta el concentrador de que el contador está apagado y qué hace en ese momento? Indique los tipos de paquetes PRIME que se observan en este proceso.
4. En las pruebas anteriores el *sniffer* ZPM está funcionando como nodo terminal. Sin embargo, también puede funcionar como *switch*. Promocione el ZPM para que pase a actuar como *switch*. ¿Qué secuencia de mensajes PRIME se observan en este proceso? Una vez el ZPM ha promocionado a *switch*, ¿cuántas balizas se observan en la red PRIME?
5. Encienda a continuación los contadores. ¿Hay alguno que comunique a través del *switch*? ¿Es posible que esto ocurra en el panel? Razone adecuadamente su respuesta en base al funcionamiento del protocolo PRIME.
6. Ahora degrade el ZPM para que pase a actuar como contador. ¿Cuál es la secuencia de mensajes que se observa?
7. Con todos los contadores encendidos, vamos a capturar el espectro de frecuencia utilizando el ZPM. ¿En qué rango de frecuencias podemos ver que trabaja PRIME? ¿En

qué unidades se representa el espectro? ¿Cuál es el nivel asociado al ruido de fondo?
¿Cuál es el nivel asociado a la señal PRIME?

8. Utilizando el ZPM, indique qué modulación de las consideradas en PRIME están utilizando contadores y concentrador para comunicarse.

3.2.3.2 Bloque 2: PRIME/DLMS/COSEM e Interfaz Web del Concentrador ZIV

En este segundo bloque nos centraremos en comprender el funcionamiento del protocolo de capa de aplicación DLMS/COSEM y en explorar algunas de las posibilidades que nos ofrece la interfaz web del concentrador ZIV. Por ello haremos uso de las herramientas XLM Translator y OBIS Helper para decodificar los mensajes DLMS/COSEM capturados mediante ZIV PRIME Manager al solicitar diferentes informes mediante la interfaz web del concentrador.

Encendemos ahora todos los contadores y accedemos a la interfaz web del concentrador ZIV.

- 1.** ¿Dónde podemos ver los contadores que hay registrados en esta herramienta? ¿Cómo se identifica cada uno de ellos?
- 2.** Uno de los informes más importantes para las distribuidoras es el S02 (perfil de carga diario). Desde la interfaz web del concentrador, solicitamos un informe S02 a cualquiera de los contadores. Con ZIV PRIME Manager podemos ver el intercambio de mensajes entre este contador y el concentrador. Identifique dicha secuencia de mensajes PRIME.
- 3.** Una vez ha identificado la secuencia de mensajes PRIME, apoyándose en la herramienta XML Translator, identifique la secuencia de mensajes DLMS/COSEM indicando su relación con la secuencia de mensajes PRIME.
- 4.** En qué mensaje DLMS/COSEM se indica el informe solicitado. ¿Qué código se utiliza para ello? Traduzca el código usado en este caso utilizando para ello la herramienta OBIS Helper.
- 5.** Otro de los informes que resulta de gran importancia para las distribuidoras es el S05 (facturación diaria). Sin embargo, solicitar tanto este informe como cualquier otro a cada uno de los contadores por separado resulta muy poco eficiente, y hacerlo a todos al mismo tiempo de manera manual cada cierto tiempo también lo es, sobre todo si tenemos en cuenta el volumen de contadores que manejan las distribuidoras. Por ello, la interfaz web del concentrador nos ofrece la posibilidad de programar tareas para grupos

de contadores y que estas se realicen de manera automática cada cierto tiempo. Programe un informe S05 cada 2 minutos para los cuatro contadores físicos e identifique, capturando mediante ZPM, la primera realización de dicha tarea para cada uno de los contadores. Señale además si el informe se solicita de manera simultánea a todos los contadores (*broadcast*) o de manera secuencial.

6. Solicitamos al concentrador, también desde la interfaz web, un informe S11, que nos muestra la topología de la red y, una vez ejecutado, lo abrimos. ¿Cuántos contadores hay registrados? ¿Cuántos niveles lógicos hay en la red? ¿En base al estudio realizado en el Bloque 1, cree que se podría aumentar el número de niveles lógicos de la red?

7. Ahora solicitamos un informe G02 (estadísticas diarias de comunicación con contadores) al concentrador. ¿Qué porcentajes se observan en dicho informe? ¿Qué mecanismo PRIME cree que se utiliza para calcular estas estadísticas de comunicación?

3.2.3.3 Bloque 3: Comunicaciones extremo a extremo (PRIME/DLMS/COSEM + STG-DC) y Plataforma de Telegestión IRIS

En el último bloque nos centraremos en el protocolo de servicios web STG-DC y, sobre todo, en analizar el potencial de la plataforma de telegestión IRIS. Para ello se analizarán las diferentes posibilidades que ofrece.

Accedemos ahora a la Plataforma de Telegestión IRIS.

1. ¿Qué información observa en la pestaña Panel de control? ¿A qué se refiere: a una red en concreto o toda la infraestructura telegestionada?

2. Vaya a la pestaña Concentradores → Todos los Concentradores y seleccione el concentrador ZIV del panel.

- a. Seleccione la pestaña Propiedades y analice la información disponible. En esta pestaña suelen aparecer lo que las eléctricas llaman “contadores saltarines”, que son contadores que no están conectados a ese CT sino a uno cercano, pero que aun así se comunican con él. ¿A qué fenómeno se debe esto?
- b. Otra de las pestañas sobre las que nos gustaría llamar la atención es la de Eventos. Uno de los Eventos más utilizados por las distribuidoras es el de detección de fraude. En base a lo visto anteriormente, ¿cómo cree que el CNC puede detectar dichos fraudes?

3. Vaya a la pestaña Contadores y seleccione un contador ZIV del panel. Seleccione la pestaña Propiedades y analice la información disponible. ¿Qué información observa que aparece para los contadores y no lo hace en el caso de los concentradores?

4. Vaya a la pestaña colecciones. ¿Cuál es la diferencia entre una colección de usuario y una colección de sistema? ¿Para qué podrían resultar útiles las colecciones?

5. Marcando uno o varios concentrador/es en la lista de todos los concentradores nos aparece el botón Acciones. De entre las acciones permitidas, seleccionamos Realizar Operación y solicitamos un informe S24, que muestra la tabla de contadores de la red PRIME. Analice la pila de protocolos del tráfico capturado mediante Wireshark. ¿Qué mensajes son los que nos indican la solicitud y el envío de este informe? Analice también la información que incluye el informe S24 descargándolo a través de IRIS.

6. Otras de las opciones que aparecen en la pestaña acciones son “Eliminar concentrador” y “Eliminar del grid”. ¿Cuál es la diferencia entre eliminar un concentrador del sistema y eliminarlo del grid?

7. ¿Por qué motivos cree que una distribuidora puede decidir eliminar un concentrador del sistema? Haciendo uso de IRIS, elimine primero un concentrador virtual y después el concentrador físico ZIV (panel) del sistema. Analice el intercambio de mensajes que involucra esta operación usando Wireshark. ¿Qué ocurre con los contadores asociados a este concentrador (panel) en IRIS? Haciendo uso de IRIS, comisione el concentrador físico de ZIV de nuevo. ¿Qué ocurre con los contadores huérfanos anteriormente asociados a este concentrador en IRIS después del comisionado? Analice el intercambio de mensajes que involucra esta operación e indique en base a qué informe realiza IRIS el comisionado automático de los contadores huérfanos.

Nota: Se aconseja añadir a una colección algunos de los contadores asociados al concentrador que se va a eliminar para poder ver su estado después de eliminar dicho concentrador.

8. Seleccione un contador activo de la lista del concentrador físico, vaya a la pestaña Operaciones y ordene configurar la potencia máxima (B02). Elija una de las tarifas disponibles. Antes de aplicar el cambio, ponga ZIV PRME Manager a capturar. ¿Qué secuencia de mensajes PRIME se intercambia para llevar a cabo dicho cambio? Identifique también el intercambio de mensajes STG-DC asociado a esta operación en la captura de Wireshark. Indique qué otras operaciones permite realizar la plataforma IRIS sobre los contadores.

9. Vaya a la pestaña Propiedades de ese contador y elimínelo. ¿Qué secuencia de mensajes observamos en ZIV PRIME Manager? ¿Qué observa en el contador al finalizar dicho proceso? ¿Es equivalente a apagar un contador? ¿Cuál es la diferencia?

¿Qué mensajes STG-DC asociados a esta operación observa en la captura de Wireshark?

10. Suponga que se va a cerrar un comercio y la distribuidora quiere cortar el suministro del local sin necesidad de apagar el contador para, en un futuro, poder reanudar el suministro de manera remota, ¿cuál es la orden que tendrá que ejecutarse sobre el contador de dicho comercio para que se produzca un corte de suministro? Ejecute dicha orden e identifíquela en el intercambio de mensajes PRIME entre el contador y el concentrador.

11. Transcurrido un tiempo, el establecimiento cambia de propietario y vuelve a abrir sus puertas, por lo que la distribuidora tiene que reanudar el suministro, ¿cuál será la orden se deberá aplicar sobre el contador? Ejecute también esta orden e identifíquela capturando de nuevo mediante ZIV PRIME Manager.

12. En la pestaña “Contadores” del concentrador físico, seleccionando la opción Ver contadores en vista general se pueden marcar uno o varios contadores para realizar acciones sobre ellos (a través del botón Acciones que aparece en la parte inferior). Seleccione todos los contadores físicos y solicite un informe S02. ¿Qué diferencias se observan con ZIV PRIME Manager con respecto a cuándo solicitamos el informe a un solo contador? Identifique también el intercambio de mensajes STG-DC asociado a esta operación en la captura de Wireshark.

13. Desde IRIS, ordene una telecarga de firmware a los contadores ZIV1 y ZIV2. Analice la secuencia de mensajes PRIME utilizando la captura de ZIV PRIME Manager. ¿Cómo se realiza la telecarga de firmware: en modo *unicast*, *multicast* o *broadcast*? Razone los pros y los contras de cada opción y explique por qué cree que se utiliza el modo observado. Identifique y analice también el intercambio de mensajes STG-DC asociado a esta operación en la captura de Wireshark.

14. Vuelva a pedir un informe S02 para uno de los contadores de la red física y detenga la tarea que aparece en IRIS mientras está en curso. ¿Se observa algún tipo de mensaje PRIME en ZIV PRIME Manager que nos indique esta interrupción o tarea fallida?

15. Una de las características que diferencian a IRIS es que permite geolocalizar los dispositivos de la infraestructura telegestionada. Seleccione un concentrador y vaya a la pestaña de Geolocalización. ¿Qué información nos proporciona esta herramienta/vista? ¿Para qué cree que puede ser útil para la distribuidora? ¿En base a qué informe cree que se puede construir este mapa?

Capítulo 4

Resultados y evaluación

En este capítulo se detalla el resultado de las diferentes pruebas realizadas sobre la infraestructura ciber-física, con el objetivo de dar una visión clara sobre su potencial. Para ello, se analizará el resultado de cada prueba de manera clara e ilustrativa.

4.1 Solucionario del manual de prácticas

4.1.1 Bloque 1: Protocolo PRIME y ZIV PRIME Manager

1. Con todos los contadores apagados, ¿qué tipos de paquetes PRIME se observan? ¿Para qué sirve cada uno de ellos? ¿Hay alguno que llame especialmente la atención? En caso de que sea así, ¿a qué cree que se debe?

Inicialmente, podemos observar balizas procedentes del nodo base (BPDUs) al resto de la subred, cuyo objetivo es proporcionar información de la estructura de la trama MAC y del acceso al canal al resto de dispositivos de la subred.

```
[RX] 2016-07-11 17:55:53 4028.943452(0.011008) dbpsk_f rxpow:6.74693(Vrms) evm:13.1(dB) channels:phy0
Beacon: sna:40:40:22:02:27:be sid:0 level:0 cnt:1 slt:0 seq:5 frq:0 NEW SNA
00 | 27 00 20 00 00 28 40 40 22 02 27 be 00 00 9b 37
10 | 39 1f
[RX] 2016-07-11 17:55:53 4029.561696(0.011008) dbpsk_f rxpow:6.83989(Vrms) evm:13.9(dB) channels:phy0
Beacon: sna:40:40:22:02:27:be sid:0 level:0 cnt:1 slt:0 seq:6 frq:0 delta:+0.000004
00 | 27 00 20 00 00 30 40 40 22 02 27 be 00 00 0d 30
10 | 21 f7
[RX] 2016-07-11 17:55:54 4030.179944(0.011008) dbpsk_f rxpow:6.72369(Vrms) evm:13.9(dB) channels:phy0
Beacon: sna:40:40:22:02:27:be sid:0 level:0 cnt:1 slt:0 seq:7 frq:0 delta:+0.000008
00 | 27 00 20 00 00 38 40 40 22 02 27 be 00 00 83 72
10 | 22 c2
```

Figura 41 – Secuencia de BPDUs

Dado que todos los contadores están apagados, sería de esperar que no hubiera más tráfico. Sin embargo, se observan mensajes de *keep-alive* entre el concentrador y el *sniffer* (ALV_S y ALV_B), debido a que este último está configurado como nodo de servicio en ZIV PRIME manager.

Estos mensajes sirven para varias cosas, como por ejemplo sacar estadísticas de comunicaciones o detectar cuándo un nodo de servicio abandona la red. Su funcionamiento se basa en un contador que cada nodo de servicio inicia en el momento de registrarse en la subred (en el campo **REG.TIME**) que se reinicia cada vez que este nodo recibe un mensaje **ALV_B** con el valor fijado en el campo **ALV.TIME**, momento en el que se genera un mensaje de respuesta **ALV_S** para indicar que está activo. Si el contador expira, el nodo base asume que el nodo de servicio ha abandonado la red y procede a cancelar su registro. Asimismo, cada *switch* en el camino de un mensaje **ALV_B** guarda el valor de este contador, de modo que si no recibe un mensaje **ALV_S** del nodo de destino en el tiempo fijado por este contador, se procede al des-registro del dicho nodo por parte del nodo base.

2. Ahora encendemos uno de los contadores. ¿Qué tipo de mensajes PRIME se observan? ¿Para qué sirve cada uno de ellos? ¿En qué mensaje asigna el concentrador el NID (SID + LNID) al contador?

Al encender uno de los contadores, además de los mensajes anteriormente mencionados, se aprecia la secuencia de mensajes típica del proceso de registro. Dicho registro se lleva a cabo mediante los siguientes mensajes:

- **REG_REQ:** solicitud de registro por parte del contador (con EUI-48 40:40:22:89:1c:53) al concentrador o nodo base (SID: 0).
- **REG_RSP:** respuesta y aceptación de la solicitud por parte del concentrador. En él se lleva a cabo la asignación del NID (SID+LNID) al contador.
- **REG_ACK:** reconocimiento del registro por parte del contador.

```
[RX] 2016-07-11 17:56:37 4073.590900(0.013248) dbpsk_f rxpow:5.52244(Vrms) evm:12.9(dB) channels:phy0
GPDU: sna:40:40:22:02:27:be UP level:0 frametime:0.133956 SCP
REG_REQ: eui48: 40:40:22:89:1c:53 sid:0 spc:0 caps:0x45
00 | 00 00 5e 06 01 00 ff fc 08 02 28 40 40 22 89 1c
10 | 53 8a 07 5e 9a
[RX] 2016-07-11 17:56:37 4073.671668(0.013248) dbpsk_f rxpow:6.60526(Vrms) evm:12.9(dB) channels:phy0
GPDU: sna:40:40:22:02:27:be DO level:0 frametime:0.214724 SCP
REG_RSP: eui48: 40:40:22:89:1c:53 sid:0 lnid:11040 spc:0 caps:0x47 time:0
00 | 00 40 99 06 01 00 ac 80 08 02 38 40 40 22 89 1c
10 | 53 d0 49 b3 a3
[RX] 2016-07-11 17:56:37 4073.702640(0.013248) dbpsk_f rxpow:5.62633(Vrms) evm:12.9(dB) channels:phy0
GPDU: sna:40:40:22:02:27:be UP level:0 frametime:0.245696 SCP
REG_ACK: eui48: 40:40:22:89:1c:53 sid:0 lnid:11040 spc:0 caps:0x45 time:0
00 | 00 00 5e 06 01 00 ac 80 08 02 28 40 40 22 89 1c
10 | 53 74 64 62 36
```

Figura 42 – Secuencia PRIME de registro

Inmediatamente después de que el proceso de registro se haya completado comienza el proceso de conexión, mediante los siguientes mensajes de control:

- **CON_REQ_S:** solicitud de conexión por parte del contador. En este mensaje se establece el LCID, en este caso con valor 256, lo que implica que la conexión ha sido solicitada por el nodo de servicio (el contador). Los valores del LCID entre 0 y 255 indican que la conexión es solicitada por el nodo base, mientras que los valores entre 256 y 511 indican que la solicitud procede de un nodo de servicio.
- **CON_REQ_B:** respuesta y aceptación de la conexión por parte del concentrador.

```
[RX] 2016-07-11 17:56:38 4074.488560(0.015488) dbpsk_f rxpow:6.36544(Vrms) evm:12.4(dB) channels:phy0
GPDU: sna:40:40:22:02:27:be UP level:0 frametime:0.413368 SCP
CON_REQ_S: sid:0 lnid:11040 lcid:256 type:3 arg:y
00 | 00 00 5e 06 02 00 ac 80 11 21 00 03 0d 5a 49 56
10 | 30 30 34 32 35 34 30 31 31 35 15 57 48 da
[RX] 2016-07-11 17:56:38 4074.549368(0.013248) dbpsk_f rxpow:6.59054(Vrms) evm:12.9(dB) channels:phy0
GPDU: sna:40:40:22:02:27:be DO level:0 frametime:0.474176 SCP
CON_REQ_B: sid:0 lnid:11040 lcid:256 type:3 arg:y
00 | 00 40 99 06 02 00 ac 80 08 21 00 03 04 00 80 00
10 | 00 2b 5d 4b 27
```

Figura 43 - Secuencia PRIME de conexión

Una vez establecida la conexión ya podemos visualizar el intercambio de mensajes *keep-alive* entre el concentrador y el contador que se acaba de conectar.


```
[RX] 2016-07-11 17:56:53 4089.679864(0.011008) dbpsk_f rxpow:6.72098(Vrms) evm:14.1(dB) channels:phy0
GPDU: sna:40:40:22:02:27:be DO level:0 frametime:0.148604 SCP
ALV_B: sid:0 lnid:11040 rxcnt:0 txcnt:1 ssid:255 time:0
00 | 00 40 99 06 07 00 ac 80 03[04 00 ff]31 f1 4c 5d
[RX] 2016-07-11 17:56:53 4089.710620(0.011008) dbpsk_f rxpow:5.61055(Vrms) evm:12.9(dB) channels:phy0
GPDU: sna:40:40:22:02:27:be UP level:0 frametime:0.179360 SCP
ALV_S: sid:0 lnid:11040 rxcnt:1 txcnt:1 ssid:255 time:0
```

Figura 44 – Intercambio de mensajes PRIME para el proceso de keep-alive

3. Apagamos ahora el contador. ¿Qué mecanismo tiene el concentrador para detectar si un contador está encendido o apagado? ¿Cómo (o cuándo) se da cuenta el concentrador de qué el contador está apagado y qué hace en ese momento? Indique los tipos de paquetes PRIME que se observan en este proceso.

Como se ha mencionado anteriormente, el mecanismo que tiene el concentrador o nodo base para detectar que un contador ha dejado de tener conectividad es el intercambio de mensajes *keep alive*. Si el concentrador no recibe ningún mensaje **ALV_S** del contador en el intervalo de tiempo fijado por el campo **ALV.TIME** da por hecho que se encuentra apagado y procede a cancelar su registro de la subred. La **Figura 45** muestra el último mensaje **ALV_S** que recibe el concentrador.

```
[RX] 2016-07-11 17:56:53 4089.679864(0.011008) dbpsk_f rxpow:6.72098(Vrms) evm:14.1(dB) channels:phy0
GPDU: sna:40:40:22:02:27:be DO level:0 frametime:0.148604 SCP
ALV_B: sid:0 lnid:11040 rxcnt:0 txcnt:1 ssid:255 time:0
00 | 00 40 99 06 07 00 ac 80 03[04 00 ff]31 f1 4c 5d
[RX] 2016-07-11 17:56:53 4089.710620(0.011008) dbpsk_f rxpow:5.61055(Vrms) evm:12.9(dB) channels:phy0
GPDU: sna:40:40:22:02:27:be UP level:0 frametime:0.179360 SCP
ALV_S: sid:0 lnid:11040 rxcnt:1 txcnt:1 ssid:255 time:0
```

Figura 45 – Intercambio de mensajes PRIME para el proceso de keep-alive

Como podemos ver el campo **ALV.TIME** tiene valor 0 que, como se indica en el estándar y como puede verse en la Tabla 11, equivale a un intervalo de 32 segundos. Como se muestra en la **Figura 45**, el concentrador recibe el último **ALV_S** a las 17:56:53.

ALV.TIME	3 bits	Time to wait for ALV_B messages before assuming the service node has been unregistered by the base node. ALV.TIME = 0 => 32 seconds ALV.TIME = 1 => 64 seconds ALV.TIME = 2 => 128 seconds ~ 2.1 minutes ALV.TIME = 3 => 256 seconds ~ 4.2 minutes ALV.TIME = 4 => 512 seconds ~ 8.5 minutes ALV.TIME = 5 => 1024 seconds ~ 17.1 minutes ALV.TIME = 6 => 2048 seconds ~ 34.1 minutes ALV.TIME = 7 => 4096 seconds ~ 68.3 minutes
----------	--------	--

Tabla 11 – Posibles valores del campo **ALV.TIME** [8]

Cuando los 32 segundos expiran, el concentrador procede a cancelar el registro del contador en la subred, como se aprecia en la **Figura 46**.

```
[RX] 2016-07-11 17:57:25 4121.783336(0.013248) dbpsk_f rxpow:6.68262(Vrms) evm:12.9(dB) channels:phy0
GPDU: sna:40:40:22:02:27:be DO level:0 frametime:0.103444 SCP
REG_UNR_B: eui48: 40:40:22:89:1c:53 sid:0 lnid:11040
00 | 00 40 99 06 01 00 ac 80 08[80 00 40 40 22 89 1c
10 | 53]43 65 21 01
```

Figura 46 – Mensaje PRIME de desregistro

El mensaje utilizado para llevar a cabo esta cancelación de registro es el **REG_UNR_B**, que puede tener lugar después de un mensaje **REG_UNR_S** si es el nodo de servicio quien solicita la cancelación de registro o, como en este caso, ir solo ya que es el nodo base quien la lleva a cabo al considerar que el contador se encuentra apagado. También es posible comprobar que, efectivamente, desde el último mensaje **ALV_S** hasta que se lleva a cabo la cancelación del registro han pasado exactamente 32 segundos (17:56:53 – 17:57:25).

4. En las pruebas anteriores el *sniffer* ZPM está funcionando como nodo terminal. Sin embargo, también puede funcionar como *switch*. Promocione el ZPM para que pase a actuar como *switch*. ¿Qué secuencia de mensajes PRIME se observa en este proceso? Una vez el ZPM ha promocionado a *switch*, ¿cuántas balizas se observan en la red PRIME?

El proceso de promoción a *switch* del *sniffer* lleva más tiempo que los procesos vistos anteriormente. En primer lugar, el *sniffer* envía una solicitud de promoción al concentrador mediante un mensaje **PRO_REQ_S**.

```
[TX] 2016/11/02 18:59:53 12804.466968(0.013248) dbpsk_f channels:1
GPDU: sna:40:40:22:02:27:be UP level:0
PRO_REQ_S: sid:0 lnid:9791 rq:0 caps:0x6 pna:00:29:23:be:84:e1 upcost:4 dncost:4 time:0
00 | 00 00 05 e6 03 00 98 fc 0b[00 ff 00 29 23 be 84
10 | e1 04 04 06]38 e8 0a 9b
```

Figura 47 – Mensaje PRIME de solicitud de promoción

Al cabo de cierto tiempo el concentrador confirma dicha solicitud mediante un mensaje **PRO_REQ_B**, al que sigue el mensaje **PRO_ACK** por parte del *sniffer*.

```
[RX] 2016/11/02 19:00:23 12834.571772(0.011008) dbpsk_f rxpow:6.74289(Vrms) evm:13.7(dB) channels:phy0
GPDU: sna:40:40:22:02:27:be DO level:0 frametime:0.162764 SCP
PRO_REQ_B: sid:0 lnid:9791 nsid:1 time:0
00 | 00 40 99 06 03 00 98 fc 02[00 01]40 82 13 05
[TX] 2016/11/02 19:00:24 12834.595768(0.011008) dbpsk_f channels:1
GPDU: sna:40:40:22:02:27:be UP level:0
PRO_ACK: sid:0 lnid:9791 nsid:1 time:0
00 | 00 00 05 e6 03 00 98 fc 02[00 01]88 34 61 e5
```

Figura 48 – Secuencia PRIME de respuesta y reconocimiento de promoción

A continuación, observamos mensajes de control BSI (*Beacon Slot Information*), ya que ahora hay un nuevo nodo *switch* en la subred y estos mensajes sirven para intercambiar información que será utilizada por un *switch* para transmitir su baliza. De este modo, el concentrador, para notificar los cambios en los *beacon slots*, envía un mensaje **BSI_IND** al nuevo nodo *switch* para aumentar el número de *slots* y asignarle

un *slot* para la transmisión de sus BPDUs. En este mensaje también se incluye la frecuencia de transmisión de balizas que tendrá este nuevo *switch*. El *switch* responde con un **BSI_ACK**.

```
[RX] 2016/11/02 19:00:24 12834.698124(0.011008) dbpsk_f rxpow:6.80230(Vrms) evm:13.5(dB) channels:phy0
GPDU: sna:40:40:22:02:27:be DO level:0 frametime:0.289116 SCP
BSI_IND: sid:0 lnid:9791 frq:3 slt:2 seq:0
00 | 00 40 99 06 04 00 98 fc 02[03 40]ea 4b 24 d6
[TX] 2016/11/02 19:00:24 12834.724024(0.011008) dbpsk_f channels:1
GPDU: sna:40:40:22:02:27:be UP level:0
BSI_ACK: sid:0 lnid:9791 frq:3 slt:2 seq:0
00 | 00 00 5e 06 04 00 98 fc 02[03 40]22 fd 56 36
```

Figura 49 – Mensajes PRIME para notificar cambios en las balizas

Como podemos ver, en el mensaje **BSI_IND** se establecen tanto la frecuencia de transmisión de balizas del *switch* como el *slot* que ocuparan dichas balizas (*slot* 2, estando el *slot* 0 reservado para el nodo base). La frecuencia de transmisión tiene valor 3, que en el estándar se indica que equivale a una baliza por cada 8 tramas, siendo 0 el valor reservado para las balizas del nodo base que se transmiten en todas las tramas. La **Figura 50** muestra las equivalencias de los distintos valores posibles para la frecuencia de transmisión según el estándar.

BCN.FRQ	3 bits	Transmission frequency of this BPDUs. Values are interpreted as follows: 0 = 1 beacon every frame 1 = 1 beacon every 2 frames 2 = 1 beacon every 4 frames 3 = 1 beacon every 8 frames 4 = 1 beacon every 16 frames 5 = 1 beacon every 32 frames 6 = Reserved by ITU-T 7 = Reserved by ITU-T.
---------	--------	--

Figura 50 – Posibles frecuencias de transmisión de balizas

Una vez que el *sniffer* ha promocionado a *switch*, si capturamos tráfico podemos ver sus balizas. Éstas se diferencian de las del nodo base en los campos **BCN.LEVEL**, que indica el nivel en el que se encuentra el *switch* transmisor; **BCN.SID**, que indica el identificador del *switch* transmisor; y los ya mencionados **BCN.SLT** y **BCN.FRQ**, que indican el *slot* en el que se transmitirá la baliza del *switch* y la frecuencia de transmisión de dichas balizas respectivamente.

En la captura mostrada en la **Figura 51** aparecen dos BPDUs, de las cuales la primera corresponde al concentrador y la segunda al nuevo *switch*, de modo que podemos apreciar las diferencias en sus campos, tal y como se ha mencionado anteriormente:

```

[RX] 2016/11/03 15:36:46 1121.843976(0.011008) dbpsk_f rxpow:6.72716(Vrms) evm:13.7(dB) channels:phy0
Beacon: sna:40:40:22:02:27:be sid:0 level:0 cnt:3 slt:0 seq:7 frq:0 delta:+0.000004
00 | 27 00 60 00 00 38 40 40 22 02 27 be 00 00 7a 0b
10 | fe f5
[TX] 2016/11/03 15:36:47 1122.446772(0.011008) dbpsk_f channels:
Beacon: sna:40:40:22:02:27:be sid:4 level:1 cnt:3 slt:2 seq:8 frq:3
00 | 26 04 68 00 01 43 40 40 22 02 27 be 04 04 ae 70
10 | 02 e0

```

Figura 51 – Valores de los campos de las BPDUs

El campo **BCN.LEVEL** indica el nivel 1, es decir, el nivel inmediatamente inferior al nodo base, que es donde se encuentra el *switch*. El **SID** tiene valor 4, a diferencia del **SID** del nodo base que tiene valor 0. El *slot* que ocuparán las balizas y su frecuencia de transmisión también varían, como se ha indicado anteriormente.

5. Encienda a continuación los contadores. ¿Hay alguno que comunique a través del *switch*? ¿Es posible que esto ocurra en el panel? Razone adecuadamente su respuesta en base al funcionamiento del protocolo PRIME.

Al encender los contadores podemos observar que todos ellos comunican a través del nodo base (concentrador) y ninguno lo hace a través del *switch*. En la red sobre la que estamos trabajando, nunca sucederá esto ya que las distancias entre contadores y concentrador son muy pequeñas y todos los contadores reciben las balizas del concentrador, por lo que no tienen necesidad de llegar al concentrador a través de un *switch* intermedio.

6. Ahora degrade el ZPM para que pase a actuar como contador. ¿Cuál es la secuencia de mensajes que se observa?

Al degradar el *sniffer*, este envía una solicitud de degradación al nodo base, como ilustra la **Figura 52**, y realiza dicha degradación de forma autónoma, sin necesidad de respuesta del concentrador debido a que no hay ningún nodo que se conecte a la subred a través de él y, por tanto, es innecesario que se encuentre en estado de *switch*. Del mismo modo, aunque no lo degrademos manualmente, el *sniffer* se degradará automáticamente al cabo de un tiempo por los mismos motivos.

```

[RX] 2016/11/09 13:15:20 8929.873592(0.011008) dbpsk_f rxpow:6.58594(Vrms) evm:16.9(dB) channels:phy0
GPDU: sna:40:40:22:02:27:be UP level:0 frametime:0.036636 SCP
PRO_DEM_S: sid:0 lnid:9835 nsid:1 time:0
00 | 00 00 5e 06 03 00 99 ac 02[80 01]65 b2 63 06

```

Figura 52 – Mensaje PRIME de solicitud de degradación

7. Con todos los contadores encendidos, vamos a capturar el espectro de frecuencia utilizando el ZPM. ¿En qué rango de frecuencias podemos ver que trabaja PRIME? ¿En qué unidades se representa el espectro? ¿Cuál es el nivel asociado al ruido de fondo? ¿Cuál es el nivel asociado a la señal PRIME?

PRIME soporta actualmente rangos de frecuencia que van desde la banda CENELEC-A (3-95 KHz) hasta los 500 KHz. En este caso en particular vemos que está trabajando en un rango de frecuencias comprendido aproximadamente entre 40-90 KHz (PRIME opera en la banda 41-89 KHz en su versión 1.3.6).

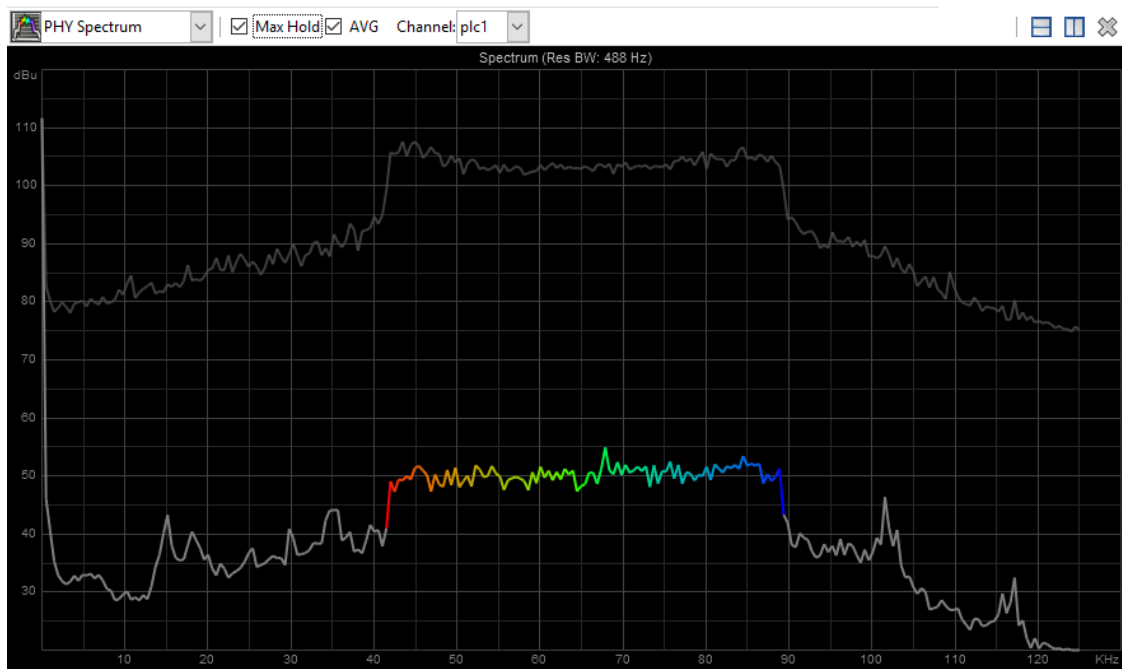


Figura 53 – Rango de frecuencias PRIME

La representación del espectro se realiza en dBu (cuyo nivel de referencia son 0.7746 V) en función de la frecuencia. La señal PRIME tiene un nivel máximo asociado entre 100 y 110 dBu.

8. Utilizando el ZPM, indique qué modulación de las consideradas en PRIME están utilizando contadores y concentrador para comunicarse.

En el estándar de PRIME se consideran 3 posibles modulaciones: DBPSK, DQPSK y D8PSK, cuyas respectivas constelaciones se muestran en la **Figura 54**.

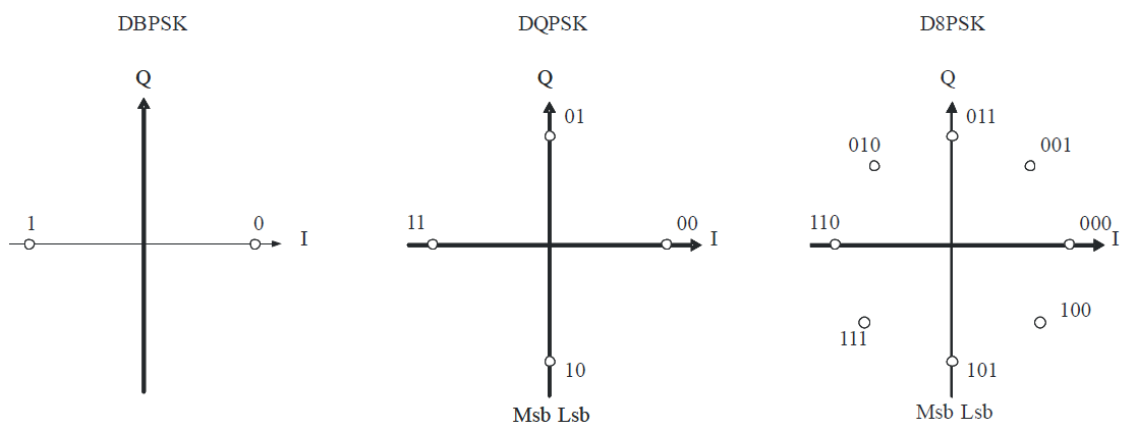


Figura 54 – Modulaciones posibles en PRIME

ZIV PRIME Manager muestra la siguiente constelación:

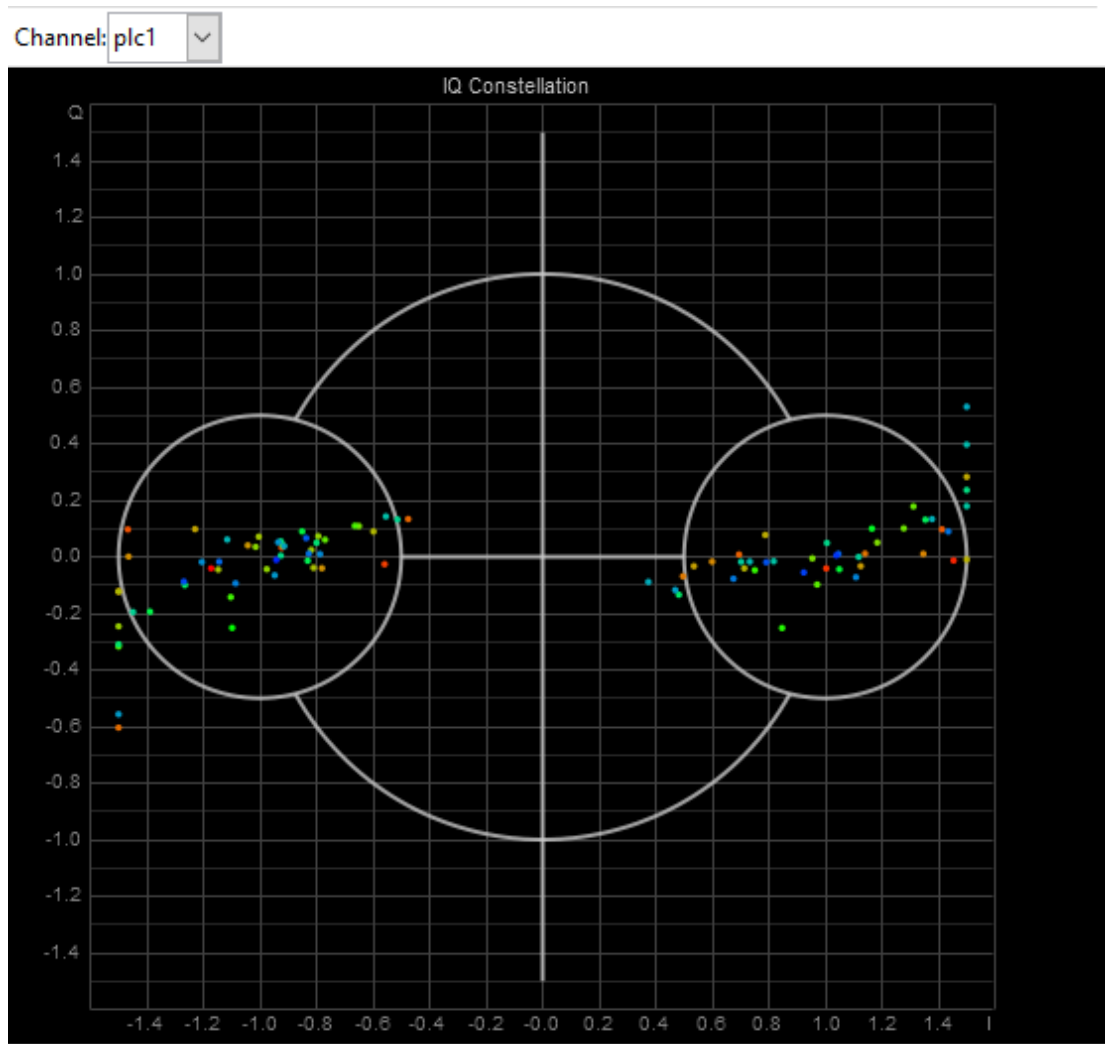


Figura 55 – Constelación PRIME utilizada

Esta constelación coincide con la anteriormente mostrada para la modulación DBPSK, por lo que los contadores y el concentrador de la red física PRIME utilizan modulación DBPSK.

4.1.2 Bloque 2: PRIME/DLMS/COSEM e Interfaz Web del Concentrador ZIV

1. ¿Dónde podemos ver los contadores que hay registrados en esta herramienta? ¿Cómo se identifica cada uno de ellos? El concentrador tiene asociado un contador interno, que ejerce de supervisor y que podemos desactivar y activar, obteniendo los diferentes valores sumados de todos los concentradores de la subred asociada a dicho concentrador, ¿para qué cree que puede ser de utilidad este contador interno?

Podemos ver la lista de contadores en la pestaña “*Operation*” → “*Meter list*”. Éstos aparecen identificados por su número de serie y su dirección MAC. También se indica si se encuentran activos o no.

El contador interno, como se menciona, ejerce de supervisor, obteniendo los valores de potencia y facturación de la subred del concentrador completa. Las mediciones obtenidas por dicho contador interno deben coincidir con la suma de las mediciones individuales de cada contador, teniendo en cuenta la diferencia lógica y acotada previamente a causa de las pérdidas en la transmisión (conocidas como pérdidas técnicas). Por tanto, este contador interno resulta útil como método para detectar distintos tipos de fraude, que quedarán de manifiesto en caso de detectarse anomalías en la comparación de mediciones.

2. Uno de los informes más importantes para las distribuidoras es el S02. Desde la interfaz web del concentrador, solicitamos un informe S02 (perfil de carga diario) a cualquiera de los contadores. Con ZIV PRIME Manager podemos ver el intercambio de mensajes entre este contador y el concentrador. Identifique dicha secuencia de mensajes PRIME.

La información se envía en forma de mensajes PRIME de tipo *Data*, que son los mensajes utilizados para transmitir MAC PDUs, que se identifican fácilmente desde el momento en el que solicitamos el informe hasta su finalización, como ilustra la **Figura 56**.

```

[RX] 2016/11/15 15:35:15 8350.336352(0.011008) dbpsk_f rxpow:7.16646(Vrms) evm:14.2(dB) channels:phy0
Beacon: sna:40:40:22:02:27:be sid:0 level:0 cnt:1 slt:0 seq:21 frq:0 delta:-0.000004
00 | 27 00 20 00 00 a8 40 40 22 02 27 be 00 00 59 1f
10 | e7 f7
[RX] 2016/11/15 15:35:15 8350.409336(0.033408) dbpsk_f rxpow:7.25112(Vrms) evm:16.5(dB) channels:phy0
GPDU: sna:40:40:22:02:27:be DO level:0 frametime:0.072984 SCP
DATA sid:0 lcid:12808 lcid:256
00 | 00 40 99 05 00 00 c8 20 3f[c0 90 00 00 90 01 02
10 | 60 36 a1 09 06 07 60 85 74 05 08 01 01 8a 02 07
20 | 80 8b 07 60 85 74 05 08 02 01 ac 0a 80 08 30 30
30 | 30 30 30 30 30 31 be 10 04 0e 01 00 00 00 06 5f
40 | 1f 04 00 00 10 14 00 fd]47 70 05 65
[RX] 2016/11/15 15:35:15 8350.474040(0.028928) dbpsk_f rxpow:6.69581(Vrms) evm:12.7(dB) channels:phy0
GPDU: sna:40:40:22:02:27:be UP level:0 frametime:0.137688 SCP
DATA sid:0 lcid:12808 lcid:256
00 | 00 00 5e 05 00 00 c8 20 32[c0 90 01 00 90 02 01
10 | 61 29 a1 09 06 07 60 85 74 05 08 01 01 a2 03 02
20 | 01 00 a3 05 a1 03 02 01 00 be 10 04 0e 08 00 06
30 | 5f 1f 04 00 00 10 14 00 fc 00 07]a6 40 1f c6

```

Figura 56 – Secuencia de mensajes PRIME de tipo Data

3. Una vez ha identificado la secuencia de mensajes PRIME, apoyándose en la herramienta XML Translator, identifique la secuencia de mensajes DLMS/COSEM indicando su relación con la secuencia de mensajes PRIME.

DLMS/COSEM es el protocolo de capa de aplicación de PRIME, más concretamente DLMS es el protocolo de capa de aplicación y COSEM es el modelo de datos. ZIV PRIME Manager solamente captura tráfico de mensajes PRIME, por lo que no tenemos una visión directa de los mensajes DLMS/COSEM contenidos dentro de las tramas PRIME. Los mensajes DLMS/COSEM se presentan a nivel PRIME como el *payload* de mensajes de tipo Data, aunque no guardan relación directa en términos de longitud, es decir, un mensaje DLMS/COSEM no está contenido necesariamente en un mensaje PRIME de tipo Data, sino que puede estar dividido en varios en caso de tener un tamaño más grande que la máxima MSDU permitida en PRIME (256 bytes).

Para decodificar mensajes DLMS/COSEM mediante XML Translator primero tenemos que identificar el paquete que transporta la MAC PDU. La estructura de una MAC PDU es la siguiente:

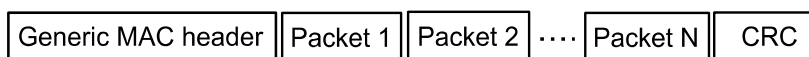


Figura 57 – Estructura de una MAC PDU genérica

En este caso la MAC PDU transporta un solo paquete, que podemos identificar entre corchetes en la secuencia de bytes. La estructura de un paquete es la siguiente:

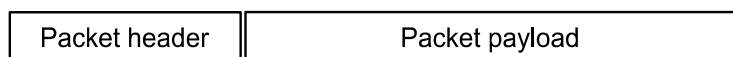


Figura 58 – Estructura del payload de una GPDU

Queremos identificar la carga útil (*payload*) para después decodificarla. La carga útil del paquete va inmediatamente después de la cabecera, que ocupa los primeros 7

bytes (primera línea). Dentro de esta carga útil debemos identificar la secuencia inicial de bytes que identifica a cada tipo de mensaje DLMS/COSEM. Esta secuencia se encuentra siempre al principio del *payload* (3 primeros bytes). Tenemos que introducir a partir de esta secuencia hasta el final de la carga útil (final del contenido entre corchetes) en XML Translator, sin incluir la columna de la izquierda que indica la posición relativa (dentro de la trama) del primer octeto de cada fila.

Sin embargo, esta traducción no siempre resulta tan trivial, ya que en ocasiones un sólo mensaje DLMS/COSEM será dividido en diferentes tramas a nivel PRIME, debido a que resulta demasiado grande para enviarlo solamente en una. En este caso tendremos que concatenar los bytes pertenecientes al *payload* de las diferentes tramas PRIME en las que se divide el mensaje en cuestión. Hay, sin embargo, una particularidad a la hora de concatenar, ya que a partir de la segunda trama solo deben descartarse los primeros 4 bytes del paquete, al contrario de lo que sucede en la primera trama, donde se descartan los 7 primeros bytes. Una vez se hayan concatenado las diferentes tramas, se introduce la secuencia de bytes en el XML Translator y obtendremos la traducción a XML. Para identificar dónde empieza y acaba el mensaje DLMS/COSEM y cuantas tramas PRIME comprende solamente hay que fijarse en el sentido (UP o DO) de las tramas (ascendente si es de contador a concentrador y descendente si es de concentrador a contador), ya que el primer mensaje en el que cambie el sentido implicará el fin del mensaje anterior. Por ejemplo, en el caso mostrado en la **Figura 59**, las dos primeras tramas tienen sentido descendente y la tercera ascendente, por lo que las dos primeras tramas componen un mensaje DLMS/COSEM y la tercera forma parte de otro mensaje distinto.

```
[RX] 2016/11/15 15:35:15 8350.585584(0.024448) dbpsk_f rxpow:7.20665(vr
GPDU: sna:40:40:22:02:27:be DO level:0 frametime:0.249232 SCP
DATA sid:0 lnid:12808 lcld:256
00 | 00 40 99 05 00 00 c8 20 26[81 90 01 01 90 01 02
10 | c0 01 c1 00 07 01 00 63 01 00 ff 02 01 01 02 04
20 | 02 04 12 00 08 09 06 00 00 01 00 00 ff 0f 02]3d
30 | 1a 74 75
[RX] 2016/11/15 15:35:15 8350.618632(0.024448) dbpsk_f rxpow:7.07407(vr
GPDU: sna:40:40:22:02:27:be DO level:0 frametime:0.282280 SCP
DATA sid:0 lnid:12808 lcld:256
00 | 00 40 99 05 00 00 c8 20 25[c2 90 01 80 12 00 00
10 | 09 0c 07 e0 0b 0e 01 0f 2a 2f 00 80 00 00 09 0c
20 | 07 e0 0b 0f 02 0f 2a 2f 00 80 00 00 01 00]11 98
30 | e2 34
[RX] 2016/11/15 15:35:15 8350.858692(0.011008) dbpsk_f rxpow:6.99753(vr
GPDU: sna:40:40:22:02:27:be UP level:0 frametime:0.522340 SCP
DATA sid:0 lnid:12808 lcld:256
00 | 00 00 5e 05 00 00 c8 20 03[81 90 03]76 76 e9 c5
```

Figura 59 – Identificación en las tramas PRIME del final de un mensaje DLMS/COSEM y comienzo del siguiente

Una vez detallada la manera en la que se decodifican las tramas de bytes DLMS/COSEM, pasamos a analizar el intercambio de mensajes. En primer lugar, se produce el establecimiento de la asociación de aplicación (AA), lo cual se realiza mediante el servicio COSEM-OPEN, cuyas primitivas son transportadas por las PDUs de capa de aplicación (APDUs) AARQ y AARE. El primer mensaje DLMS/COSEM que se envía, por tanto, es una AARQ (**AssociationRequest**) del cliente (concentrador) al servidor (contador), es decir, una petición de establecimiento de una AA entre ambos.

La secuencia de bytes que identifica a una AARQ es “60 36 a1”. La AARQ es seguida por una AARE (**AssociationResponse**), cuya secuencia inicial es “61 29 a1”, en la que se acepta la asociación por parte del servidor.

```
[RX] 2016/11/15 15:35:15 8350.409336(0.033408) dbpsk_f rxpow:7.25112(vrms) evm:16.5(dB) channels:phy0
GPDU: sna:40:40:22:02:27:be DO level:0 frametime:0.072984 SCP
DATA sid:0 lrid:12808 lcid:256
00 00 40 99 05 00 00 c8 20 3f c0 90 00 00 90 01 02
10 60 36 a1 09 06 07 60 85 74 05 08 01 01 8a 02 07
20 80 8b 07 60 85 74 05 08 02 01 ac 0a 80 08 30 30
30 30 30 30 30 30 31 be 10 04 0e 01 00 00 00 06 5f
40 1f 04 00 00 10 14 00 fd 47 70 05 65
[RX] 2016/11/15 15:35:15 8350.474040(0.028928) dbpsk_f rxpow:6.69581(vrms) evm:12.7(dB) channels:phy0
GPDU: sna:40:40:22:02:27:be UP level:0 frametime:0.137688 SCP
DATA sid:0 lrid:12808 lcid:256
00 00 00 5e 05 00 00 c8 20 32 c0 90 01 00 90 02 01
10 61 29 a1 09 06 07 60 85 74 05 08 01 01 a2 03 02
20 01 00 a3 05 a1 03 02 01 00 be 10 04 0e 08 00 06
30 5f 1f 04 00 00 10 14 00 fc 00 07 a6 40 1f c6
```

Figura 60 – Identificación de las secuencias iniciales de los mensajes DLMS/COSEM AssociationRequest y AssociationResponse

La decodificación mediante XML Translator es la que nos permite identificar el tipo de mensaje en caso de que no conozcamos el mensaje DLMS/COSEM asociado a la secuencia inicial de bytes. Para la secuencia que comienza con “60 36 a1” obtenemos, como se ha indicado antes, el mensaje **AssociationRequest**:

```
<AssociationRequest>
  <ApplicationContextName Value="LN" />
  <SenderACSERequirements Value="1" />
  <MechanismName Value="LOW_SECURITY" />
  <CallingAuthenticationValue Value="3030303030303031" />
  <InitiateRequest>
    <ProposedDlmsVersionNumber Value="06" />
    <ProposedConformance>
      <ConformanceBit Name="SelectiveAccess" />
      <ConformanceBit Name="Get" />
      <ConformanceBit Name="BlockTransferWithGetOrRead" />
    </ProposedConformance>
    <ProposedMaxPduSize Value="00FD" />
  </InitiateRequest>
</AssociationRequest>
```

Figura 61 – Decodificación en XML de un mensaje DLMS/COSEM AssociationRequest

Podemos diferenciar los diferentes campos del mensaje **AssociationRequest**, entre los que destacan:

- El campo **ApplicationContextName** define el contexto mediante el cual tiene lugar el intercambio de datos con el contador, que puede ser LN (*Logical Name*) o SN (*Short Name*), y que difieren entre sí en la forma en la que los datos son referenciados (o direccionados). En el contexto LN los datos son referenciados mediante el código OBIS (nombre lógico). Este contexto no puede ser elegido por el cliente, sino que es fijado por el fabricante del contador.
- El campo **ProposedDlmsVersionNumber**, actualmente está fijado a 6 que es el número de versión del protocolo DLMS.
- El campo **ProposedConformance** es una lista de las capacidades que se espera que tenga el contador.

- El campo **ProposedMaxPduSize** indica el máximo tamaño de PDU que el cliente es capaz de almacenar. En este caso este valor está fijado a 253 bytes. El valor FFFF significa que no hay límite.

Para la secuencia que comienza con “61 29 a1”, obtenemos el mensaje **AssociationResponse**:

```
<AssociationResponse>
  <ApplicationContextName Value="LN" />
  <AssociationResult Value="00" />
  <ResultSourceDiagnostic>
    <ACSEServiceUser Value="00" />
  </ResultSourceDiagnostic>
  <InitiateResponse>
    <NegotiatedDlmsVersionNumber Value="06" />
    <NegotiatedConformance>
      <ConformanceBit Name="SelectiveAccess" />
      <ConformanceBit Name="Get" />
      <ConformanceBit Name="BlockTransferWithGetOrRead" />
    </NegotiatedConformance>
    <NegotiatedMaxPduSize Value="00FC" />
    <VaasName Value="0007" />
  </InitiateResponse>
</AssociationResponse>
```

Figura 62 – Decodificación en XML de un mensaje DLMS/COSEM AssociationResponse

En este caso podemos diferenciar los siguientes campos principales:

- El campo **AssociationResult** indica si la asociación se ha producido con éxito, en cuyo caso el valor será cero.
- El campo **NegotiatedConformance** incluye una lista de capacidades que implementa el contador, que son las que hemos solicitado en el mensaje **AssociationRequest**, excepto aquellas que no son soportadas por el contador.
- El campo **NegotiatedMaxPduSize** indica la longitud máxima de PDU que el contador puede almacenar. El cliente nunca debe enviar PDUs mayores que este valor.

Una vez que se ha establecido la asociación, se utiliza el servicio GET para leer el valor de uno o más objetos COSEm. Hay diferentes variantes de **GetRequest** y la más simple es el **GetRequestNormal**. El concentrador solicita el informe al contador mediante un mensaje **GetRequestNormal** (secuencia inicial “c0 01 c1”). El servicio GET se utiliza para leer el valor de uno o más objetos COSEM, por lo que el mensaje **GetRequest** es una petición de lectura. Este mensaje es dividido en diferentes tramas a nivel PRIME, por lo que la traducción se realizará conforme se ha detallado anteriormente.

```

[RX] 2016/11/15 15:35:15 8350.585584(0.024448) dbpsk_f rxpow:7.20665(vrms) evm:15.0(dB) channels:phy0
GPDU: sna:40:40:22:02:27:be DO level:0 frametime:0.249232 SCP
DATA sid:0 lrid:12808 lcid:256
00 | 00 40 99 05 00 00 c8 20 26[81 90 01 01 90 01 02
10 | c0 01 c1 00 07 01 00 63 01 00 ff 02 01 01 02 04
20 | 02 04 12 00 08 09 06 00 00 01 00 00 ff 0f 02]3d
30 | 1a 74 75
[RX] 2016/11/15 15:35:15 8350.618632(0.024448) dbpsk_f rxpow:7.07407(vrms) evm:14.9(dB) channels:phy0
GPDU: sna:40:40:22:02:27:be DO level:0 frametime:0.282280 SCP
DATA sid:0 lrid:12808 lcid:256
00 | 00 40 99 05 00 00 c8 20 25[c2 90 01 80 12 00 00
10 | 09 0c 07 e0 0b 0e 01 0f 2a 2f 00 80 00 00 09 0c
20 | 07 e0 0b 0f 02 0f 2a 2f 00 80 00 00 01 00]11 98
30 | e2 34

```

*Figura 63 – Identificación de la secuencia inicial de un mensaje DLMS/COSEM
GetRequestNormal*

La decodificación nos indica el mensaje **GetRequestNormal** y sus diferentes campos:

```

<GetRequest>
  <GetRequestNormal>
    <InvokeIdAndPriority Value="C1" />
    <AttributeDescriptor>
      <ClassId Value="0007" />
      <InstanceId Value="0100630100FF" />
      <AttributeId Value="02" />
    </AttributeDescriptor>
    <AccessSelection>
      <AccessSelector Value="01" />
      <AccessParameters>
        <Structure Qty="04">
          <Structure Qty="04">
            <LongUnsigned Value="0008" />
            <OctetString Value="0000010000FF" />
            <Integer Value="02" />
            <LongUnsigned Value="0000" />
          </Structure>
          <OctetString Value="07E00B0E010F2A2F00800000" />
          <OctetString Value="07E00B0F020F2A2F00800000" />
          <Array Qty="00">
            </Array>
          </Structure>
        </AccessParameters>
      </AccessSelection>
    </GetRequestNormal>
  </GetRequest>

```

Figura 64 – Decodificación en XML de un mensaje DLMS/COSEM AssociationResponse

- El campo **InvokeIdAndPriority** es un valor de byte. El bit en la posición 7 indica la prioridad, donde 1 significa alta prioridad. El resto de bits solamente identifican al mensaje **GetRequestNormal**.
- El campo **AttributeDescriptor** contiene 3 elementos:
 - **ClassId** es el identificador de clase del objeto que aloja el atributo que queremos leer.
 - **InstanceId** es el código OBIS del objeto, que nos indica qué tipo de información se está solicitando. Para el informe S02 el OBIS es "01 00 63 01 00 FF", como podemos ver en la **Figura 64**.
 - **AttributeId** es el número de atributo del atributo que queremos leer.

En el caso de que se solicite más información al contador con un nuevo **GetRequestNormal**, el último octeto de su secuencia inicial aumentará de manera

secuencial, pasando a ser esta secuencia “c0 01 c2”, “c0 01 c3”, y así sucesivamente hasta el final del intercambio de información.

La respuesta al **GetRequestNormal** puede ser un **GetResponseNormal**, en el que se envían los datos solicitados, o un **GetResponseWithDataBlock**. En muchos casos, el **GetRequestNormal** resultaría en una PDU de un gran tamaño. Cuando esto sucede, el contador enviará los datos solicitados en varias tramas PRIME dividiendo la información en bloques mediante mensajes **GetResponseWithDataBlock**. Esta característica se denomina transferencia de bloques y es un mecanismo de segmentación de datos soportado en la capa de aplicación, con el objetivo de adaptar el protocolo DLMS/COSEM a PRIME.

La secuencia inicial de este mensaje es “c4 02 c1”, que se corresponde con un mensaje **GetResponseWithDataBlock** y es la misma durante toda la transferencia de la información segmentada en bloques, es decir, hasta que el concentrador solicita nueva información mediante un nuevo **GetRequestNormal**. De este modo, los datos solicitados se enviarán en diferentes bloques. En caso de no conocer con qué mensaje se corresponde esta secuencia inicial, esto quedará claro a la hora de traducirlo a XML.

```
[RX] 2016/11/15 15:35:15 8351.021624(0.026688) dbpsk_f rxpow:6.88241(vrms) evm:12.2(dB) channels:phy0
GPDU: sna:40:40:22:02:27:be UP level:0 frametime:0.067028 SCP
DATA sid:0 lrid:12808 lcrid:256
00 | 00 00 5e 05 00 00 c8 20 2f[81 90 03 05 90 02 01
10 | c4 02 c1 00 00 00 00 01 00 81 f1 01 18 02 08 09
20 | 0c 07 e0 0b 0e 01 10 00 00 00 80 00 00 11 00 06
30 | 00 00 00 00 06 00 00 00]27 2c 2a c1
[RX] 2016/11/15 15:35:15 8351.060012(0.026688) dbpsk_f rxpow:6.81531(vrms) evm:12.0(dB) channels:phy0
GPDU: sna:40:40:22:02:27:be UP level:0 frametime:0.105416 SCP
DATA sid:0 lrid:12808 lcrid:256
00 | 00 00 5e 05 00 00 c8 20 2f[82 90 03 40 00 06 00
10 | 00 00 00 06 00 00 00 00 06 00 00 00 00 06 00 00
20 | 00 00 02 08 09 0c 07 e0 0b 0e 01 11 00 00 00 80
30 | 00 00 11 02 06 00 00 00]6e 88 25 b1
[RX] 2016/11/15 15:35:15 8351.098012(0.026688) dbpsk_f rxpow:6.95260(vrms) evm:12.4(dB) channels:phy0
GPDU: sna:40:40:22:02:27:be UP level:0 frametime:0.143416 SCP
DATA sid:0 lrid:12808 lcrid:256
00 | 00 00 5e 05 00 00 c8 20 2f[83 90 03 41 00 06 00
10 | 00 00 00 06 00 00 00 00 06 00 00 00 00 06 00 00
20 | 00 00 06 00 00 00 00 02 08 09 0c 07 e0 0b 0e 01
30 | 12 00 00 00 80 00 00 11]eb 64 96 68
```

*Figura 65 – Identificación de la secuencia inicial de un mensaje DLMS/COSEM
GetResponseWithDataBlock*

A la hora de introducir en XML Translator la secuencia completa de bytes que forman el mensaje DLMS/COSEM vemos que es una secuencia de un tamaño bastante grande (en la imagen anterior no aparece el mensaje completo, se utilizan un gran número de tramas a nivel PRIME). XML Translator arroja el siguiente resultado:

```

<GetResponse>
  <GetResponseWithDataBlock>
    <InvokeIdAndPriority Value="C1" />
    <Result>
      <LastBlock Value="00" />
      <BlockNumber Value="00000001" />
      <Result>
        <RawData Value="01180208090C07E00B0E011000000080000011000600000000" />
      </Result>
    </Result>
  </GetResponseWithDataBlock>
</GetResponse>

```

Figura 66 – Decodificación en XML de un mensaje DLMS/COSEM AssociationResponse

Como podemos ver coincide con un mensaje **GetResponseWithDataBlock**. El campo **Result** de este mensaje está compuesto por 3 elementos:

- **LastBlock** es un booleano que nos indica si se trata del último bloque de información o no (00 = false).
- **BlockNumber** es el valor que indica el número de secuencia de este bloque.
- **RawData** es una cadena de octetos que contiene los primeros n bytes de nuestros datos (la parte de los datos contenida en el primer bloque).

Si la información se transmitiera en un solo mensaje, sin ser necesario segmentarla en varios, la respuesta sería un **GetResponseNormal**, con secuencia inicial “c4 01 c1”. Para siguientes mensajes **GetResponseNormal** en los que se envíe diferente información solicitada el último octeto de la secuencia inicial aumentaría secuencialmente, de la misma forma que en el caso del mensaje **GetRequest**.

El siguiente mensaje en orden secuencial al **GetResponseWithDataBlock** ha de ser necesariamente un **GetRequestForNextDataBlock**, en el que el concentrador solicita al contador que envíe el siguiente bloque de datos. Su secuencia inicial es “c0 02 c1” y es un mensaje de un tamaño pequeño (14 bytes).

```

[RX] 2016/11/15 15:35:16 8351.319904(0.015488) dbpsk_f rxpow:7.22700(Vrms) evm:15.2(dB) channels:phy0
GPDU: sna:40:40:22:02:27:be DO level:0 frametime:0.365308 SCP
DATA sid:0 lrid:12808 lcrid:256
00 | 00 40 99 05 00 00 c8 20 0e[c3 90 07 00 90 01 02
10 | c0 02 c1 00 00 00 01]9d 8f dc f7

```

Figura 67 – Identificación de la secuencia inicial de un mensaje DLMS/COSEM GetRequestForNextDataBlock

```

<GetRequest>
  <GetRequestForNextDataBlock>
    <InvokeIdAndPriority Value="C1" />
    <BlockNumber Value="00000001" />
  </GetRequestForNextDataBlock>
</GetRequest>

```

Figura 68 – Decodificación en XML de un mensaje DLMS/COSEM GetRequestForNextDataBlock

El campo más relevante en el **GetRequestForNextDataBlock** es el campo **BlockNumber**, que indica el último bloque recibido y, por tanto, el que se espera recibir a continuación.

Esta secuencia de mensajes DLMS/COSEM (**GetResponseWithDataBlock** seguido de **GetRequestForNextDataBlock**) se repite hasta que llegamos a un **GetResponseWithDataBlock** cuyo campo **LastBlock** tiene valor 01 (01 = true), lo que nos indica que es el último bloque de datos de ese mensaje DLMS/COSEM que el contador envía al concentrador.

```
<GetResponse>
  <GetResponseWithDataBlock>
    <InvokeIdAndPriority Value="C1" />
    <Result>
      <LastBlock Value="01" />
      <BlockNumber Value="00000005" />
    </Result>
    <Result>
      <RawData Value="0208090C07E00B0F020C00000000000011000600000000060" />
    </Result>
  </GetResponseWithDataBlock>
</GetResponse>
```

Figura 69 – Último bloque de datos perteneciente a un único mensaje DLMS/COSEM enviado por el contador

En el caso de que el contador envíe más información al concentrador utilizando transferencia de bloques, el último octeto de la secuencia inicial para los siguientes mensajes **GetResponseWithDataBlock** irá aumentado secuencialmente (“c4 02 c2”, “c4 02 c3”, etc.), manteniéndose la misma secuencia durante toda la transferencia de bloques que sigue al **GetRequestNormal**, como se ha indicado anteriormente.

Una vez terminada la transferencia de bloques tiene lugar la liberación o abandono de la asociación. En primer lugar, tiene lugar la solicitud de liberación de la asociación del concentrador al contador mediante el mensaje **ReleaseRequest** (RLRQ), cuya secuencia inicial es “62 00”. Como consecuencia de esta petición del concentrador, el contador enviará un mensaje **ReleaseResponse** con secuencia inicial “63 03 80”.

```
[RX] 2016/11/15 15:35:18 8353.737928(0.013248) dbpsk_f rxpow:7.11799(Vrms) evm:14.9(dB) channels:phy0
GPDU: sna:40:40:22:02:27:be DO level:0 frametime:0.310356 SCP
DATA sid:0 lrid:12808 lcid:256
00 | 00 40 99 05 00 00 c8 20 09[c7 90 1e 00 90 01 02
10 | 62 00 03 62 6f 99
[RX] 2016/11/15 15:35:18 8353.769420(0.015488) dbpsk_f rxpow:7.00988(Vrms) evm:11.6(dB) channels:phy0
GPDU: sna:40:40:22:02:27:be UP level:0 frametime:0.341848 SCP
DATA sid:0 lrid:12808 lcid:256
00 | 00 00 5e 05 00 00 c8 20 0c[de 90 08 00 90 02 01
10 | 63 03 80 01 00]96 16 fd 06
```

Figura 70 – Identificación de las secuencias iniciales de los mensajes DLMS/COSEM ReleaseRequest y ReleaseResponse

El resultado en XML para ambos mensajes es el siguiente:


```
<ReleaseRequest>
</ReleaseRequest>
```

Figura 71 – Decodificación en XML de un mensaje DLMS/COSEM ReleaseRequest

```
<ReleaseResponse>
  <Reason Value="Normal" />
</ReleaseResponse>
```

Figura 72 – Decodificación en XML de un mensaje DLMS/COSEM ReleaseResponse

Con el mensaje **ReleaseResponse** termina la solicitud y envío del informe S02.

Siempre es posible identificar ciertos elementos de los mensajes DLMS/COSEM sin necesidad de traducir la secuencia hexadecimal a XML, ya que siempre se encuentran en la misma posición de la trama.

Por ejemplo, en el **GetRequestNormal** podemos identificar el código OBIS fácilmente, ya que siempre llevará la misma posición en la trama:

00	00	40	99	05	00	00	c8	20	26	81	90	01	01	90	01	02
10	c0	01	c1	00	07	01	00	63	01	00	ff	02	01	01	02	04
20	02	04	12	00	08	09	06	00	00	01	00	00	ff	0f	02	3d
30	1a	74	75													

Figura 73 – Identificación del código OBIS en la trama PRIME

En la secuencia de bytes que compone el mensaje **GetResponseWithDataBlock** se identifican también con facilidad el valor del campo **LastBlock** (1) y **BlockNumber** (2):

00	00	00	5e	00	00	00	c8	20	2f	81	90	03	05	90	02	01
10	c4	02	c1	00	00	00	00	01	00	81	f1	01	18	02	08	09
20	0c	07	e0	0b	0e	01	10	00	00	80	00	00	11	00	06	
30	00	00	00	00	06	00	00	00	27	2c	2a	c1				

Figura 74 – Identificación de los campos DLMS/COSEM LastBlock y BlockNumber en la trama PRIME

Por tanto, una vez familiarizados con todos los tipos de mensajes DLMS/COSEM y sus diferentes campos, es posible identificar dicho mensaje conociendo la secuencia inicial de bytes que lo identifica y el valor de sus campos sabiendo la posición de éstos en la trama.

4. ¿En qué mensaje DLMS/COSEM se indica el informe solicitado? ¿Qué código se utiliza para ello? Traduzca el código usado en este caso utilizando para ello la herramienta OBIS Helper.

Como se menciona anteriormente en el análisis de los diferentes mensajes DLMS/COSEM, el mensaje encargado de indicar el informe solicitado es el **GetRequest**, y más concretamente para este caso el **GetRequestNormal**. Dentro de

este mensaje, el código que identifica el informe es el código OBIS, contenido en el campo **InstanceId**. El código OBIS está compuesto por 6 bytes e identifica a un objeto en un dispositivo lógico de manera única.

Para la traducción del código OBIS contamos con una herramienta llamada OBIS Helper, en la que habrá que introducir los 6 bytes que lo componen en hexadecimal o en decimal, aunque en nuestro caso resulta más directo hacerlo en hexadecimal ya que es como se nos presenta la trama de datos.

Al introducir el código OBIS en hexadecimal, para lo cual hay que marcar la casilla “Hex”, y traducirlo, obtenemos la identificación del informe al que corresponde.

Para el código “01 00 63 01 00 FF” (S02) obtenemos la traducción que se muestra en la **Figura 75**.

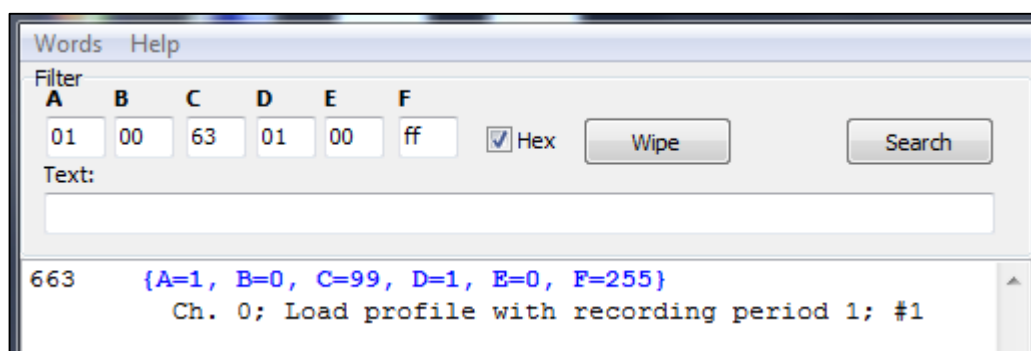


Figura 75 – Decodificación código OBIS informe S02

Como cabe esperar, OBIS Helper nos indica que este código corresponde a un informe de perfil de carga diario, es decir, un informe S02.

5. Otro de los informes que resulta de gran importancia para las distribuidoras es el S05 (facturación diaria). Sin embargo, solicitar tanto este informe como cualquier otro a cada uno de los contadores por separado resulta muy poco eficiente, y hacerlo a todos al mismo tiempo de manera manual cada cierto tiempo también lo es, sobre todo si tenemos en cuenta el volumen de contadores que manejan las distribuidoras. Por ello, la interfaz web del concentrador nos ofrece la posibilidad de programar tareas para grupos de contadores y que estas se realicen de manera automática cada cierto tiempo. Programe un informe S05 cada 2 minutos para los cuatro contadores físicos e identifique, capturando mediante ZPM, la primera realización de dicha tarea. Señale además si el informe se solicita de manera simultánea a todos los contadores o de manera secuencial.

Para programar la ejecución de tareas mediante la interfaz web del concentrador debemos ir a la sección “*Task scheduler*” y aquí programar la tarea que queramos indicando una fecha de comienzo y un periodo de ejecución (1). Para poder programar una tarea tenemos que realizar dos pasos previos. El primer paso es definir un

identificador (2), que podrá ser el mismo nombre de la tarea (S05 en este caso) para no crear confusiones, pero también cualquier otro nombre a nuestra elección y asociarlo a la tarea en que corresponda. El segundo paso es añadir los contadores sobre los que queremos que se realice la operación a esa tarea, en este caso la tarea es la solicitud de un informe S05 (3). Después de definir un identificador y añadir los dispositivos deseados a la tarea, con el periodo de tiempo y la tarea concreta programada podemos guardar los cambios.

Programmed tasks (TP TAR)

#	Task identifier (Task ID) ¹	Start time (TpHi) ²	Execution period (TpPer) ³	Priority (TpPrio) ⁴	TpCompl	
1	S02	2015/06/25,04:00:00S	1d	2	<input type="checkbox"/>	Delete
2	S04	2015/06/01,00:00:00S	1M	2	<input type="checkbox"/>	Delete
3	S05	2015/06/01,02:00:00S	00:02:00	2	<input type="checkbox"/>	Delete
4	Add					

Scheduled actions per task (TPPRO)

#	Task identifier (Task ID) ⁵	Action (TpReq) ⁶	STG send (TpSend)	Storage R/W (TpStore)	TpAttr (Query ID)	TpAt
1	S02	S02	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
2	S04	S04	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
3	S05	S05	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
4	Add					

Advanced scheduled actions per task (TPPRO)

#	Task identifier (Task ID)	Action (TpReq)	STG send (TpSend)	Storage read/write (TpStore)
1	Add			

Scheduled gas actions per task (TPPRO)

#	Task identifier (Task ID)	Action (TpReq)	STG Send (TpSend)	Storage read/write (TpStore)
1	Add			

Meters per task (TPMET)

#	Task identifier (Task ID) ⁷	Meters serial number (TpMet) ⁸	
1	S02	ZIV0042540112,ZIV0042540113,ZIV0042540114,ZIV00	Delete
2	S05	ZIV0042540112,ZIV0042540113,ZIV0042540114,ZIV00	Delete

Figura 76 – Ventana Task scheduler de la interfaz web del concentrador

La primera realización de la tarea es la siguiente:

```
[RX] 2016/11/17 17:15:53 3581.526664(0.024448) dbpsk_f rxpow:6.59015(Vrm
GPDU: sna:40:40:22:02:27:be DO level:0 frametime:0.186568 SCP
DATA sid:0 lnid:7231 lcid:256
00 | 00 40 99 05 00 00 70 fc 26[81 90 01 01 90 01 02
10 | c0 01 c1 00 07 00 00 62 02 01 ff 02 01 01 02 04
20 | 02 04 12 00 08 09 06 00 00 01 00 00 ff 0f 02]93
30 | 62 2a f7
[RX] 2016/11/17 17:15:53 3581.555380(0.024448) dbpsk_f rxpow:6.41315(Vrm
GPDU: sna:40:40:22:02:27:be DO level:0 frametime:0.215284 SCP
DATA sid:0 lnid:7231 lcid:256
00 | 00 40 99 05 00 00 70 fc 25[c2 90 01 80 12 00 00
10 | 09 0c 07 e0 0b 10 03 11 18 33 00 80 00 00 09 0c
20 | 07 e0 0b 11 04 11 18 33 00 80 00 00 01 00]93 9f
30 | d8 8f
```

Figura 77 – Primera solicitud de informe S05

Como se puede ver, el mensaje DLMS/COSEM está dividido en dos tramas a nivel PRIME. Decodificamos el mensaje para obtener el código OBIS y comprobar mediante OBIS Helper que se trata de un informe S05.

```

<GetRequest>
  <GetRequestNormal>
    <InvokeIdAndPriority Value="C1" />
    <AttributeDescriptor>
      <ClassId Value="0007" />
      <InstanceId Value="0000620201FF" />
      <AttributeId Value="02" />
    </AttributeDescriptor>
    <AccessSelection>
      <AccessSelector Value="01" />
      <AccessParameters>
        <Structure Qty="04">
          <Structure Qty="04">
            <LongUnsigned Value="0008" />
            <OctetString Value="0000010000FF" />
            <Integer Value="02" />
            <LongUnsigned Value="0000" />
          </Structure>
          <OctetString Value="07E00B100311183300800000" />
          <OctetString Value="07E00B110411183300800000" />
          <Array Qty="00">
            </Array>
          </Structure>
        </AccessParameters>
      </AccessSelection>
    </GetRequestNormal>
  </GetRequest>

```

Figura 78 – Decodificación GetRequest informe S05

Decodificamos el código OBIS mediante OBIS Helper.

OBISHelper 2.1

Words Help

Filter

A	B	C	D	E	F
00	00	62	02	01	ff

☒ Hex

Text:

492 {A=0, B=0, C=98, D=2, E=1, F=255}

Ch. 0; Data of billing period; Scheme 2; #2; Unspecified number of most recent billing periods

Figura 79 – Decodificación código OBIS de informe S05

El código OBIS nos da el informe del que se trata. Tal y como esperábamos se trata del informe S05 (facturación diaria).

6. Solicitamos al concentrador, también desde la interfaz web, un informe S11, que nos muestra la topología de la red y, una vez ejecutado, lo abrimos. ¿Cuántos contadores hay registrados? ¿Cuántos niveles lógicos hay en la red? ¿En base al estudio realizado en el Bloque 1, cree que se podría aumentar el número de niveles lógicos de la red?

Tal y como se aprecia en el informe, hay 5 contadores registrados, que aparecen identificados con el LNID con el que se registraron y conectaron en la subred. Sin embargo, uno de estos 5 contadores que aparecen en el informe es el propio *sniffer* que,

como ya se ha indicado anteriormente, se comunica con el concentrador como un contador más. Para detectar cuál de estos 5 contadores es el *sniffer*, identificamos su LNID en una captura de tráfico mediante ZPM y lo comparamos con los LNIDs del informe S11. También podría hacerse en base a su dirección MAC, ya que el informe S11 también contiene esta información. Por tanto, estrictamente sólo tenemos 4 contadores, cuya información principal viene reflejada en el informe.

```

<macListRegDevices regEntryID="40:40:22:89:1C:50"
regEntryLNID="8223" regEntryState="1" regEntryLSID="65535"
regEntrySID="0" regEntryLevel="0"/>
<macListRegDevices regEntryID="40:40:22:89:1C:51"
regEntryLNID="8568" regEntryState="1" regEntryLSID="65535"
regEntrySID="0" regEntryLevel="0"/>
<macListRegDevices regEntryID="40:40:22:89:1C:52"
regEntryLNID="8964" regEntryState="1" regEntryLSID="65535"
regEntrySID="0" regEntryLevel="0"/>
<macListRegDevices regEntryID="40:40:22:89:1C:53"
regEntryLNID="9951" regEntryState="1" regEntryLSID="65535"
regEntrySID="0" regEntryLevel="0"/>

```

Figura 80 – Informe S11

Cada dispositivo registrado en la subred debe contener la siguiente información:

- **regEntryID**: indica la dirección MAC (EUI-48) de cada contador
- **regEntryState**: indica su estado funcional actual (terminal=1, switch=2)
- **regEntryLSID** y **regEntrySID**: indican el SID y LSID de cada nodo respectivamente
- **regEntryLevel**: indica el nivel en el que se encuentra el nodo de servicio (contador)

Como podemos ver, el nivel en el que se encuentran todos los nodos de servicio en este caso es el 0, por lo que la subred solamente consta de un nivel.

Para aumentar el número de niveles lógicos de la subred, debemos promocionar al menos un dispositivo de estado terminal a *switch*, y que otros dispositivos se comuniquen con el nodo base (concentrador) a través de él. En la infraestructura sobre la que se trabaja no es posible promocionar ninguno de los contadores, sin embargo, como se ha visto en el Bloque 1, el *sniffer* se comunica con el concentrador como un contador más y es posible promocionarlo a *switch* a través de ZPM. No obstante, en este caso, es prácticamente imposible que ninguno de los contadores se comunique a través de este nuevo *switch* ya que todos ellos se encuentran en el mismo panel que el propio concentrador, por lo que su comunicación con este es óptima y siempre se comunicarán directamente con él.

7. Ahora solicitamos un informe G02 (estadísticas diarias de comunicación con contadores) al concentrador. ¿Qué porcentajes se observan en dicho informe?

¿Qué mecanismo PRIME cree que se utiliza para calcular estas estadísticas de comunicación?

El informe G02 nos muestra las estadísticas diarias de comunicación entre el concentrador y cada uno de los contadores durante un intervalo de tiempo seleccionado previamente. Estas estadísticas se muestran en forma de porcentaje de tiempo (de las 24 horas del día) durante el cual el concentrador se ha comunicado con cada contador.

```
<Report IdRpt="G02" IdPet="251530274" Version="3.1.c">
<Cnc Id="ZIV0004372798"> (1)
  <Cnt Id="ZIV0042540112"> (2)
    <G02 Fh="201611020000000000W" Atime="0" Nchanges="0"
Aconc="1440" Atimeperc="0.00" /> (3)
    <G02 Fh="201611030000000000W" Atime="127" Nchanges="2"
Aconc="1440" Atimeperc="8.82" /> (4)
    <G02 Fh="201611040000000000W" Atime="427" Nchanges="1"
Aconc="1440" Atimeperc="29.65" />
    <G02 Fh="201611050000000000W" Atime="1440" Nchanges="0"
Aconc="1440" Atimeperc="100.00" />
    <G02 Fh="201611060000000000W" Atime="1440" Nchanges="0"
Aconc="1440" Atimeperc="100.00" />
```

Figura 81 – Informe G02

Este informe muestra en primer lugar el número de serie del concentrador al que se le solicita (1) y también de cada uno de sus contadores asociados (2), de los que se mostrarán las estadísticas de comunicación. Para cada día del intervalo de tiempo seleccionado se muestra la fecha (3) y el porcentaje de tiempo en el que cada contador se está comunicando con el concentrador cada uno de los días (4). Si el porcentaje de tiempo en el que el contador y el concentrador se comunican es muy bajo (como algunos de los días mostrados en la **Figura 81**) es debido a que el contador ha estado apagado la mayoría del tiempo.

El concentrador calcula el tiempo durante el cual se está comunicando con cada contador en base a si se está produciendo intercambio de mensajes *keep-alive* entre ambos, de este modo es capaz de calcular el porcentaje de tiempo que cada contador está activo.

4.1.3 Bloque 3: Comunicaciones extremo a extremo (PRIME/DLMS/COSEM + STG) y Plataforma de Telegestión IRIS

1. ¿Qué información observa en la pestaña Panel de control? ¿A qué se refiere: a una red en concreto o toda la infraestructura telegestionada?

En la pestaña “Panel de control” se puede observar información relativa al estado de la infraestructura telegestionada. Las diferentes opciones se muestran en la parte izquierda de la pantalla.

La información (en forma de gráfico de tarta) que podemos ver en la opción “Estado de ping y PLC” es la del último ping realizado tanto a cada uno de los concentradores como a cada uno de sus contadores asociados, pudiendo diferenciar en ambos casos entre los que están activos y los que se encuentran en situación de fallo temporal o permanente.

En la opción “Listado de estadísticas” se muestra una lista más detallada de estadísticas de la infraestructura, entre las que también están las de ping, mostradas en la opción anterior. Además, también se incluye otro tipo de información como el número de concentradores que han enviado un informe S24 (lista de contadores en red PLC) o los perfiles de carga en diferentes rangos de tiempo.

La opción “Estadística de tareas” nos muestra diferentes gráficas correspondientes a 3 bloques distintos: conexiones, desconexiones y potencia máxima. En ellas se muestra el número de veces que se han llevado a cabo tareas relativas a cada una de estas tres opciones en lo que va de mes (número de conexiones y desconexiones y número de tareas de establecimiento de potencia máxima).

2. Vaya a la pestaña Concentradores → Todos los Concentradores y seleccione el concentrador ZIV del panel.

- a) Seleccione la pestaña Propiedades y analice la información disponible. En esta pestaña suelen aparecer lo que las eléctricas llaman “contadores saltarines”, que son contadores que no están conectados a ese CT sino a uno cercano, pero que aun así se comunican con él. ¿A qué fenómeno se debe esto?**

En la pestaña “Propiedades” del concentrador se muestra en primer lugar su dirección IP, el puerto de servicios web utilizado (el 8080, puerto utilizado para servicios HTTP) y una breve descripción. En esta pestaña tenemos la opción de establecer si este concentrador se encuentra habilitado, alcanzable y si se habilita o no la monitorización de ping para el cálculo de estadísticas. También podemos habilitar y deshabilitar la propiedad de Descubrimiento Automático de Dispositivos (ADD) que, de

encontrarse habilitada, implica que IRIS le pide al concentrador su lista de contadores de manera periódica para registrarlos automáticamente en el sistema. A continuación, se muestra su versión de *firmware* y de la interfaz WAN y si se encuentra comisionado. Es posible también saber si este concentrador está activo actualmente, ya que se muestra la fecha de último contacto con IRIS y la fecha del último ping realizado con el resultado del mismo. Por último, tenemos las opciones de eliminar el concentrador del sistema IRIS, mostrar las colecciones en las que se encuentra añadido y añadirlo a una nueva colección.

El suceso coloquialmente conocido como “contadores saltarines” es causado por el fenómeno del acoplamiento o diafonía, ya que así se denomina al acoplamiento cuando no es deseado, como en este caso. El acoplamiento de contador se produce cuando un contador es visto a nivel PLC por un concentrador en el que no se encuentra registrado, por lo que dicho contador es visto por más de un concentrador. Entre dos circuitos existe diafonía cuando parte de la señal de uno está presente en el otro, debido a acoplamientos magnéticos entre los elementos de ambos circuitos o como consecuencia de desequilibrios de admitancia entre sus hilos.

- b) Otra de las pestañas sobre las que nos gustaría llamar la atención es la de Eventos. Uno de los Eventos más utilizados por las distribuidoras es el de detección de fraude. En base a lo visto anteriormente, ¿cómo cree que el concentrador puede detectar dichos fraudes?**

Según lo mencionado anteriormente, el evento de fraude está relacionado con las medidas tomadas por un contador supervisor, que puede ser interno al propio concentrador o uno más de la subred. La función de este contador es la de medir la suma de todas las medidas del resto de contadores de la subred para compararla con la suma de sus medidas individuales, de modo que, si no coincide, salvando las lógicas diferencias debidas a las pérdidas técnicas (cables, etc.), se estaría ante un posible caso de fraude.

3. Vaya a la pestaña Contadores y seleccione un contador ZIV del panel. Seleccione la pestaña Propiedades y analice la información disponible. ¿Qué información observa que aparece para los contadores y no lo hace en el caso de los concentradores?

En la pestaña de “Propiedades” de un contador se muestra la información básica del mismo y, además, unas cuantas acciones que podemos realizar sobre él. En primer lugar, se muestra el concentrador PRIME al que está asociado, teniendo la posibilidad de cambiar dicho concentrador. Se indica también si el contador es o no supervisor, si está habilitado y si es alcanzable, así como su fecha y tipo de registro en la red y su versión de *firmware* tanto DLMS como PRIME. Además, desde esta pestaña podemos eliminar el contador en cuestión y mostrar las colecciones en las que se encuentra incluido, así como añadirlo a nuevas colecciones. Por último, en la parte derecha de la

pantalla se muestra la fecha y la hora de la última comprobación de estado activo del contador y las diferentes tarifas de potencia contratadas por este contador.

La información mostrada en la pestaña “Propiedades” de un concentrador es similar, si bien no idéntica, a su homóloga para un contador concreto. Sin embargo, en la pestaña “Propiedades” del concentrador no aparece ningún tipo de dato relativo a las tarifas contratadas, ya que de él dependen múltiples contadores con diferentes tarifas.

4. Vaya a la pestaña colecciones. ¿Cuál es la diferencia entre una colección de usuario y una colección de sistema? ¿Para qué podrían resultar útiles las colecciones?

La diferencia entre una colección de usuario y una colección de sistema es que las colecciones de usuario solamente son accesibles por parte del usuario que las ha creado, mientras que las colecciones de sistema tienen un carácter general y son accesibles por todos los usuarios del sistema. Así, un usuario concreto podrá acceder a todas las colecciones de sistema y a aquellas que hayan sido creadas por él mismo, pero no podrá ver las de los demás usuarios.

Las colecciones nos permiten agrupar distintos dispositivos con el fin de conseguir un mayor control sobre ellos. Pueden resultar útiles, por ejemplo, a la hora de realizar operaciones sobre contadores asociados a distintos concentradores. Resultan también de utilidad para agrupar en una misma página diferentes dispositivos que compartan alguna característica en común o con un uso más recurrente.

5. Marcando uno o varios concentrador/es en la lista de todos los concentradores nos aparece el botón Acciones. De entre las acciones permitidas, seleccione Realizar Operación y solicite un informe S24, que muestra la tabla de contadores de la red PRIME. Analice la pila de protocolos del tráfico capturado mediante Wireshark. ¿Qué tráfico es el que se captura? ¿Por qué no es tráfico STG-DC entre el concentrador e IRIS? ¿Qué deberíamos hacer para capturar este tipo de tráfico? ¿Qué mensajes son los que nos indican la solicitud y el envío de este informe? Analice también la información que incluye el informe S24 descargándolo a través de IRIS.

No podremos capturar tráfico STG-DC intercambiado entre IRIS (65.52.142.250) y el concentrador (163.117.162.240) debido a que nuestra red no es en bus, en la que todos los dispositivos comparten el mismo canal para comunicarse entre sí, sino en estrella utilizando switches, en la que los dispositivos no están directamente conectados entre sí, sino que están conectados a un punto central (switch) y todas las comunicaciones se realizan necesariamente a través de él. Por tanto, no podemos capturar tráfico STG-DC a no ser que capturásemos directamente en la puerta de enlace (163.117.162.2) o en el concentrador. Otra opción sería utilizar hubs en lugar de

switches, ya que un hub retransmite los paquetes recibidos por un puerto a todos los demás puertos por igual, al contrario que el switch, que selecciona el tráfico que pasa de un segmento a otro, de modo que sólo reenvía el paquete por el puerto oportuno para llegar a su destino. Sin embargo, estas dos opciones se descartan para este TFG ya que se trata de una red operativa y no se puede poner en riesgo su funcionamiento.

A continuación, se muestran las dos topologías mencionada (bus y estrella) siendo la de nuestra red una topología en estrella.

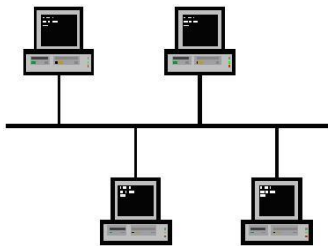


Figura 82 – Topología de red en bus

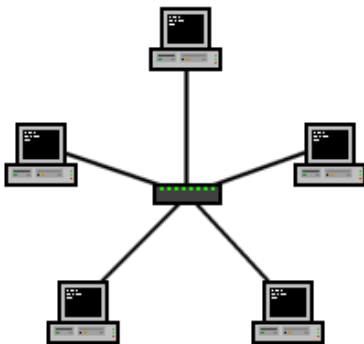


Figura 83 – Topología de red en estrella

Capturando mediante Wireshark podemos ver la secuencia de intercambio de mensajes HTTP entre el cliente web (163.117.162.246) y el servidor donde corre nuestra instancia de IRIS (65.52.142.250).

163.117.162.246	65.52.142.250	HTTP	95 POST /Iris.Platform.DeviceManager/Gateway/performListOfMetersInPLCNetworkMultiple/
65.52.142.250	163.117.162.246	TCP	60 80+53817 [ACK] Seq=1 Ack=1534 Win=513 Len=0
CiscoInc_6e:bf:17	PVST+	STP	64 RST. Root = 8192/121/00:19:a9:2f:ec:00 Cost = 7 Port = 0x804d
65.52.142.250	163.117.162.246	HTTP	516 HTTP/1.1 302 Found (text/html)
163.117.162.246	65.52.142.250	HTTP	1407 GET /Iris.Platform.DeviceManager/MyTasks HTTP/1.1
65.52.142.250	163.117.162.246	TCP	60 80+53817 [ACK] Seq=463 Ack=2887 Win=507 Len=0
65.52.142.250	163.117.162.246	TCP	1514 [TCP segment of a reassembled PDU]
65.52.142.250	163.117.162.246	TCP	1514 [TCP segment of a reassembled PDU]
65.52.142.250	163.117.162.246	TCP	1514 [TCP segment of a reassembled PDU]
163.117.162.246	65.52.142.250	TCP	54 53817+80 [ACK] Seq=2887 Ack=4843 Win=258 Len=0
65.52.142.250	163.117.162.246	TCP	1514 [TCP segment of a reassembled PDU]
65.52.142.250	163.117.162.246	TCP	1514 [TCP segment of a reassembled PDU]
65.52.142.250	163.117.162.246	TCP	1514 [TCP segment of a reassembled PDU]
65.52.142.250	163.117.162.246	TCP	1514 [TCP segment of a reassembled PDU]
65.52.142.250	163.117.162.246	TCP	1514 [TCP segment of a reassembled PDU]
163.117.162.246	65.52.142.250	TCP	54 53817+80 [ACK] Seq=2887 Ack=12143 Win=258 Len=0
65.52.142.250	163.117.162.246	TCP	1514 [TCP segment of a reassembled PDU]

Figura 84 – Captura Wireshark de solicitud y envío de informe S24

163.117.162.246	65.52.142.250	TCP	54 53817→80 [ACK] Seq=2887 Ack=26743 Win=258 Len=0
65.52.142.250	163.117.162.246	TCP	1514 [TCP segment of a reassembled PDU]
65.52.142.250	163.117.162.246	TCP	1514 [TCP segment of a reassembled PDU]
65.52.142.250	163.117.162.246	HTTP	1102 HTTP/1.1 200 OK (text/html)
163.117.162.246	65.52.142.250	TCP	54 53817→80 [ACK] Seq=2887 Ack=30711 Win=258 Len=0

Figura 85 – Captura Wireshark de final de envío de informe S24

En primer lugar, el cliente (o usuario) realiza una petición “POST” al servidor de IRIS en la que se especifica el informe que queremos solicitar, recibiendo como respuesta por parte del servidor un mensaje “302 Found”, que realiza una redirección URL e invita al usuario a realizar una nueva petición de tipo “GET” a la nueva URL especificada para obtener la información deseada del servidor. Tras enviar un ACK al cliente, el servidor inicia el envío del informe. Este informe se fracciona a nivel TCP en múltiples tramas de igual tamaño. El cliente envía un ACK al servidor cada cierto número de tramas recibidas para indicar que la recepción ha sido exitosa. En la última trama vemos el mensaje “200 OK”, la respuesta estándar para peticiones correctas en HTTP, que en realidad es enviado inmediatamente después de la petición “GET”, pero que Wireshark no es capaz de construir hasta no recibir la totalidad de las tramas. Si miramos la información que transporta la primera trama enviada por el servidor, en ASCII podemos ver el mensaje “HTTP/1.1 200 OK”.

0000	44 1e a1 df 93 ae 00 19 a9 2f ec 00 08 00 45 00	D..... ./...E.
0010	05 dc 7c 63 40 00 6e 06 74 1e 41 34 8e fa a3 75	.. c@.n. t.A4...u
0020	a2 f6 00 50 d2 39 b7 89 b5 32 fc ca b5 b2 50 10	...P.9...2....P.
0030	01 fb 91 01 00 00 48 54 54 50 2f 31 2e 31 20 32HT TP/1.1 2
0040	30 30 20 4f 4b 0d 0a 43 61 63 68 65 2d 43 6f 6e	00 OK .C ache-Con
0050	74 72 6f 6c 3a 20 70 72 69 76 61 74 65 2c 20 73	trol: pr ivate, s

Figura 86 – Vista Wireshark en hexadecimal y ASCII de la primera trama enviada del informe S24

En IRIS obtenemos la siguiente información:

Lista de Contadores de la Red PLC para el Concentrador ZIV0004372798			
Número de Serie del Contador	Activo	Estado PLC	Fecha
ZIV0042540112	Y	1	11/11/2016 18:29:34
ZIV0042540113	Y	2	11/11/2016 15:46:34
ZIV0042540114	Y	2	11/11/2016 15:46:37
ZIV0042540115	Y	2	11/11/2016 15:45:26

Figura 87 – Vista del informe S24 en IRIS

Se puede ver la lista actual de contadores del concentrador identificados por su número de serie. La columna “Estado PLC” nos indica el estado de cada uno de los contadores de la subred diferenciándose tres posibles estados:

- Activo (valor 2) → El concentrador puede comunicarse con el contador.
- Fallo temporal (valor 1) → La comunicación entre concentrador y contador se ha perdido temporalmente.

- Fallo permanente (valor 0) → Después de un intervalo de tiempo establecido en estado de fallo temporal, el concentrador pasa a encontrarse en fallo permanente.

6. Otras de las opciones que aparecen en la pestaña acciones son “Eliminar concentrador” y “Eliminar del grid”. ¿Cuál es la diferencia entre eliminar un concentrador del sistema y eliminarlo del grid?

La opción “Eliminar concentrador” elimina completamente el concentrador seleccionado del sistema de telegestión IRIS, mientras que la opción “Eliminar del grid” permite descartar de la lista de trabajo los dispositivos sobre los que no se quiere actuar, pero estos permanecen en el sistema. Por tanto, cuando eliminamos un concentrador del grid, éste ya no aparecerá junto al resto de concentrador es para realizar acciones sobre él.

7. ¿Por qué motivos cree que una distribuidora puede decidir eliminar un concentrador del sistema? Haciendo uso de IRIS, elimine primero un concentrador virtual y después el concentrador físico ZIV (panel) del sistema. Analice el intercambio de mensajes que involucra esta operación usando Wireshark. ¿Qué ocurre con los contadores asociados a este concentrador (panel) en IRIS? Haciendo uso de IRIS, comisione el concentrador físico de ZIV de nuevo. ¿Qué ocurre con los contadores huérfanos anteriormente asociados a este concentrador en IRIS después del comisionado? Analice el intercambio de mensajes que involucra esta operación e indique en base a qué informe realiza IRIS el comisionado automático de los contadores huérfanos.

Nota: Se aconseja añadir a una colección algunos de los contadores asociados al concentrador que se va a eliminar para poder ver su estado después de eliminar dicho concentrador.

Los motivos que pueden llevar a una distribuidora a eliminar un concentrador del sistema son diversos. En primer lugar, pueden querer eliminarlo debido que deje de funcionar o que su funcionamiento no sea el deseado. Otra razón es la voluntad de contar con equipamiento de una sola marca, puesto que, aunque PRIME garantiza interoperabilidad entre equipos de distintas marcas, puede darse el caso de que los dispositivos del mismo fabricante funcionen mejor entre sí.

En primer lugar, eliminamos un concentrador virtual en la pestaña “Propiedades” del propio concentrador mediante la opción “Eliminar” concentrador. Una vez se ha completado la eliminación. Después nos dirigimos a la colección en la que hemos guardado algunos de los contadores virtuales anteriormente asociados al concentrador virtual eliminado para ver el estado en el que se encuentran ahora. Todos estos contadores son ahora denominados contadores huérfanos, es decir, contadores que no están asociados a ningún concentrador. En la pestaña “Propiedades” de cualquiera de

ellos podemos ver que no se encuentra asociado a ningún concentrador y se especifica su condición de contador huérfano.



Figura 88 – Vista de un contador huérfano en IRIS

Para volver a comisionar el concentrador eliminado debemos en primer lugar añadir dicho concentrador al sistema IRIS desde la pestaña “Todos los concentradores”, añadiendo su número de serie y su URL en la opción “Añadir concentrador”. Cuando se añada este nuevo concentrador su comisionado comienza de manera automática. De este modo, los contadores anteriormente asociados a él vuelven a asociarse de manera automática.

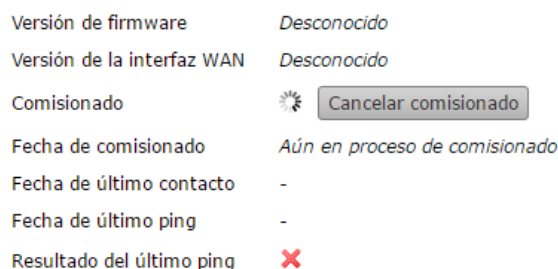


Figura 89 – Información de concentrador recién añadido a IRIS

El comisionado del concentrador es un proceso que consta de varios pasos. En primer lugar, IRIS comprueba la conectividad con el concentrador. Una vez se ha verificado dicha conectividad, IRIS averigua la versión WAN del concentrador para saber cómo tiene que llevar a cabo la comunicación con él. Por último, IRIS le solicita al concentrador su lista actual de contadores a través del informe S24 y estos son añadidos a IRIS.

8. Seleccione un contador activo de la lista del concentrador físico, vaya a la pestaña Operaciones y ordene configurar la potencia máxima (B02). Elija una de las tarifas disponibles. Antes de aplicar el cambio, ponga ZIV PRIME Manager a capturar. ¿Qué secuencia de mensajes PRIME se intercambia para llevar a cabo

dicho cambio? Analice también la secuencia de mensajes DLMS/COSEM e indique si hay algún mensaje que no haya visto anteriormente al solicitar el resto de informes. Identifique, si es posible, el intercambio de mensajes STG-DC asociado a esta operación en la captura de Wireshark. Indique qué otras operaciones permite realizar la plataforma IRIS sobre los contadores.

Capturando tráfico con ZPM, los mensajes PRIME que podemos ver son de tipo Data al igual que sucede con el resto de informes.

Al analizar la secuencia de mensajes DLMS/COSEM se pueden ver una serie de mensajes **SetRequest**, más concretamente **SetRequestNormal** (secuencia inicial “c0 01 c1”), seguidos cada uno de ellos por un mensaje **SetResponseNormal** (secuencia inicial “c5 01 c1”). Hasta ahora no nos habíamos encontrado con ningún mensaje DLMS/COSEM que utilizase el servicio SET, debido a que lo único que habíamos hecho era solicitar la lectura de datos de los contadores, para lo cual se utiliza el servicio GET (servicio para lectura de datos). Sin embargo, ahora hemos dado una orden al contador (modificar su potencia máxima) y esta orden requiere de la escritura de datos en el contador por parte del concentrador, para lo cual se utiliza el servicio SET. Aquí, a diferencia de informes como el S02, la respuesta será un mensaje **SetResponseNormal** y no habrá transferencia de bloques porque en ella no estamos enviando datos al concentrador, es una simple confirmación.

```
[RX] 2016/11/14 17:11:51 13641.519132(0.019968) dbpsk_f rxpow:7.08570(Vrms)
GPDU: sna:40:40:22:02:27:be DO level:0 frametime:0.287552 SCP
DATA sid:0 lnid:11848 lcid:256
00 | 00 40 99 05 00 00 b9 20 19[d0 90 19 00 90 01 01
10 | c1 01 c1 00 03 00 01 5e 22 0b ff 02 00 06 00 00
20 | 04 4c]83 21 4d 57
[RX] 2016/11/14 17:11:51 13641.757540(0.011008) dbpsk_f rxpow:7.12052(Vrms)
GPDU: sna:40:40:22:02:27:be UP level:0 frametime:0.525960 SCP
DATA sid:0 lnid:11848 lcid:256
00 | 00 00 5e 05 00 00 b9 20 03[99 90 11]35 04 f8 b7
[RX] 2016/11/14 17:11:51 13641.849828(0.011008) dbpsk_f rxpow:7.12154(Vrms)
Beacon: sna:40:40:22:02:27:be sid:0 level:0 cnt:1 slt:0 seq:16 frq:0 de
00 | 27 00 20 00 00 80 40 40 22 02 27 be 00 00 e7 d7
10 | d3 78
[RX] 2016/11/14 17:11:52 13641.871416(0.013248) dbpsk_f rxpow:7.00464(Vrms)
GPDU: sna:40:40:22:02:27:be UP level:0 frametime:0.021588 SCP
DATA sid:0 lnid:11848 lcid:256
00 | 00 00 5e 05 00 00 b9 20 0b[d9 90 11 00 90 01 01
10 | c5 01 c1 00]1c d5 26 0b
```

Figura 90 – Identificación de la secuencia inicial de los mensajes SetRequestNormal y SetResponseNormal

```

<SetRequest>
  <SetRequestNormal>
    <InvokeIdAndPriority Value="C1" />
    <AttributeDescriptor>
      <ClassId Value="0003" />
      <InstanceId Value="00015E220BFF" />
      <AttributeId Value="02" />
    </AttributeDescriptor>
    <Value>
      <DoubleLongUnsigned Value="0000044C" />
    </Value>
  </SetRequestNormal>
</SetRequest>

```

Figura 91 – Decodificación SetRequestNormal

```

<SetResponse>
  <SetResponseNormal>
    <InvokeIdAndPriority Value="C1" />
    <Result Value="Success" />
  </SetResponseNormal>
</SetResponse>

```

Figura 92 – Decodificación SetResponseNormal

No nos es posible ver el intercambio de mensajes STG-DC ya que cuando el concentrador (163.117.162.240) envía datos a IRIS (65.52.142.250), al estar en redes distintas, los datos se enviarán a nuestra puerta de enlace o *gateway* y desde ahí hacia fuera de nuestra red. Tal y como se ha explicado anteriormente, la única manera de poder capturar tráfico STG-DC en nuestra red (con topología en estrella) sería capturando tráfico directamente en la puerta de enlace o en el concentrador. También sería posible capturar este tráfico utilizando *hubs* en lugar de *switches* ya que los *hubs* envían el mismo tráfico por todos sus puertos.

Las operaciones que IRIS nos permite realizar sobre los contadores son muy variadas. Por un lado, están las ya vistas como solicitar diferentes informes, que se agrupan dentro de la categoría “Peticiones”. Algunos ejemplos de peticiones son los informes S02 y S05, ya conocidos, pero también hay otros como el S03 (valores absolutos diarios), S07 (informe de fallo de voltaje), S26 (datos instantáneos bajo demanda), etc. Podemos también visualizar los eventos del contador, destacando el evento de fraude. Las órdenes, como la de configurar potencia máxima (B02), son las que nos permiten modificar directamente parámetros del contador. Además de la mencionada podemos reconectar el contador (B03), desconectar contador, actualizar *firmware* de contador (B05) y controlar activación del contador (B06). Por último, también podemos visualizar el informe de curva de carga del contador.

9. Vaya a la pestaña Propiedades de ese contador y elimínelo. ¿Qué secuencia de mensajes observamos en ZIV PRIME Manager? ¿Qué observa en el contador al

finalizar dicho proceso? ¿Es equivalente a apagar un contador? ¿Cuál es la diferencia?

Eliminar un contador mediante IRIS no tiene ningún efecto en el estado de la red, simplemente se elimina del sistema IRIS y ya no puede ser telegestionado. La diferencia con apagar este contador es obvia: al apagar el contador éste deja de comunicarse con el concentrador y cesa su actividad, por lo que será imposible telegestionarlo a través de ella, mientras que al eliminarlo de IRIS todo esto se mantiene intacto y solamente es eliminado de la plataforma.

10. Suponga que se va a cerrar un comercio y la distribuidora quiere cortar el suministro del local, ¿cuál es la orden que tendrá que ejecutarse sobre el contador de dicho comercio para que se produzca un corte de suministro? Ejecute dicha orden e identifíquela en el intercambio de mensajes PRIME entre el contador y el concentrador.

La orden que nos permite cortar el suministro proporcionado por un contador es la orden B03 (desconectar contador), en la pestaña de “Operaciones” de un contador. De este modo, el contador corta el suministro que proporciona al cliente, pero sigue encendido y comunicándose de manera normal con el concentrador, a la espera de reanudar el suministro cuando reciba la orden.

11. Transcurrido un tiempo, el establecimiento cambia de propietario y vuelve a abrir sus puertas, por lo que la distribuidora tiene que reanudar el suministro, ¿cuál será la orden se deberá aplicar sobre el contador? Ejecute también esta orden e identifíquela capturando de nuevo mediante ZIV PRIME Manager.

La orden para reanudar el suministro de un contador es también la orden B03 (reconectar contador). Al recibir esta orden., el contador conmuta al estado opuesto en el que se encuentre. En el momento en el que se ejecute esta orden, el suministro se reanudará con la tarifa contratada en ese momento.

12. En la pestaña “Contadores” del concentrador físico, seleccionando la opción Ver contadores en vista general se pueden marcar uno o varios contador/es para realizar acciones sobre ellos (a través del botón Acciones que aparece en la parte inferior). Seleccione todos los contadores físicos y solicite un informe S02. ¿Qué diferencias se observan con ZIV PRIME Manager con respecto a cuándo solicitamos el informe a un solo contador? Identifique también el intercambio de mensajes STG-DC asociado a esta operación en la captura de Wireshark.

El informe se envía al concentrador de forma secuencial, cada contador envía su S02 individualmente.

En el laboratorio del grupo de investigación del Departamento de Ingeniería Telemática la red es estructurada y utiliza *switches*, por lo que para ver tráfico STG-DC tendríamos que capturar directamente en la puerta de enlace o en el concentrador o utilizar *hubs* en lugar de *switches*.

13. Desde IRIS, ordene una telecarga de *firmware* a los contadores ZIV1 y ZIV2. Analice la secuencia de mensajes PRIME utilizando la captura del ZIV PRIME Manager. ¿Cómo se realiza la telecarga de *firmware*: en modo *unicast*, *multicast* o *broadcast*? Razone los pros y contras de cada opción y explique por qué cree que se utiliza el modo observado. Identifique y analice también el intercambio de mensajes STG-DC asociado a esta operación en la captura de Wireshark.

La telecarga de *firmware* a través de IRIS se realiza en modo *unicast*. La ventaja del modo *unicast* es que permite una detección de errores más sencilla: si la actualización no se ha llevado a cabo correctamente es más sencillo detectar en qué contador o contadores se han producido errores. Además, el modo *unicast* también permite un seguimiento más sencillo de los procesos de actualización de *firmware*. La principal ventaja que tienen los modos *multicast* y *broadcast* frente a *unicast* es el consumo de ancho de banda (el mensaje de telecarga de *firmware* se envía sólo una vez) y el tiempo (al enviar los paquetes una sola vez para todos los dispositivos que se van a actualizar conseguimos que la actualización de grupos de contadores sea más rápida). Por el contrario, al realizarse en *multicast* o *broadcast* resulta mucho más difícil, en el caso de producirse errores en la actualización de *firmware* de algún contador, acotar ese error para ver en qué proceso de actualización en concreto se ha producido.

14. Vuelva a pedir un informe S02 para uno de los contadores de la red física y detenga la tarea que aparece en IRIS mientras está en curso. ¿Se observa algún tipo de mensaje PRIME en ZIV PRIME Manager que nos indique esta interrupción o tarea fallida?

Una vez que la tarea se ha iniciado, aunque la cancelemos en IRIS, esta terminará de ejecutarse normalmente. La opción que nos da IRIS es la de cancelarla mientras todavía está en espera, por lo que en ZIV PRIME Manager no veremos ningún tipo de mensaje que indique esta cancelación ya que el intercambio de mensajes entre el concentrador y el contador no se ha iniciado todavía.

Como podemos comprobar, IRIS nos permite monitorizar el curso de las tareas, no solamente mediante la posibilidad de cancelarlas, sino también ofreciéndonos información sobre su estado actual, los ficheros generados y procesados en la realización de esta tarea y permitiendo la visualización de la información resultante de la tarea.

15. Una de las características que diferencian a IRIS es que permite geolocalizar los dispositivos de la infraestructura telegestionada. Seleccione un concentrador y vaya a la pestaña de Geolocalización. ¿Qué información nos proporciona esta herramienta/vista? ¿Para qué cree que puede ser útil para la distribuidora? ¿En base a qué informe cree que se puede construir este mapa?

Desde esta pestaña podemos ver la ubicación en el mapa del concentrador en cuestión y de todos sus contadores asociados. Esta vista resulta de gran utilidad para la distribuidora ya que le permite comprobar de manera gráfica y rápida (no hace falta más que un vistazo) el estado de la red de contadores del concentrador. Los diferentes estados de los contadores se indican mediante un código de colores. Si un contador aparece en verde significa que está activo, si aparece en amarillo quiere decir que está en situación de fallo temporal, si aparece en rojo está en estado de fallo permanente y si aparece en gris no hay información sobre él.

Este mapa de estado de la red se construye en base al informe S24, que se ha detallado anteriormente, puesto que en él se incluye exactamente la misma información que aquí se representa de manera gráfica sobre el mapa.

☆ **Número de Serie del Concentrador: VDC-000001**

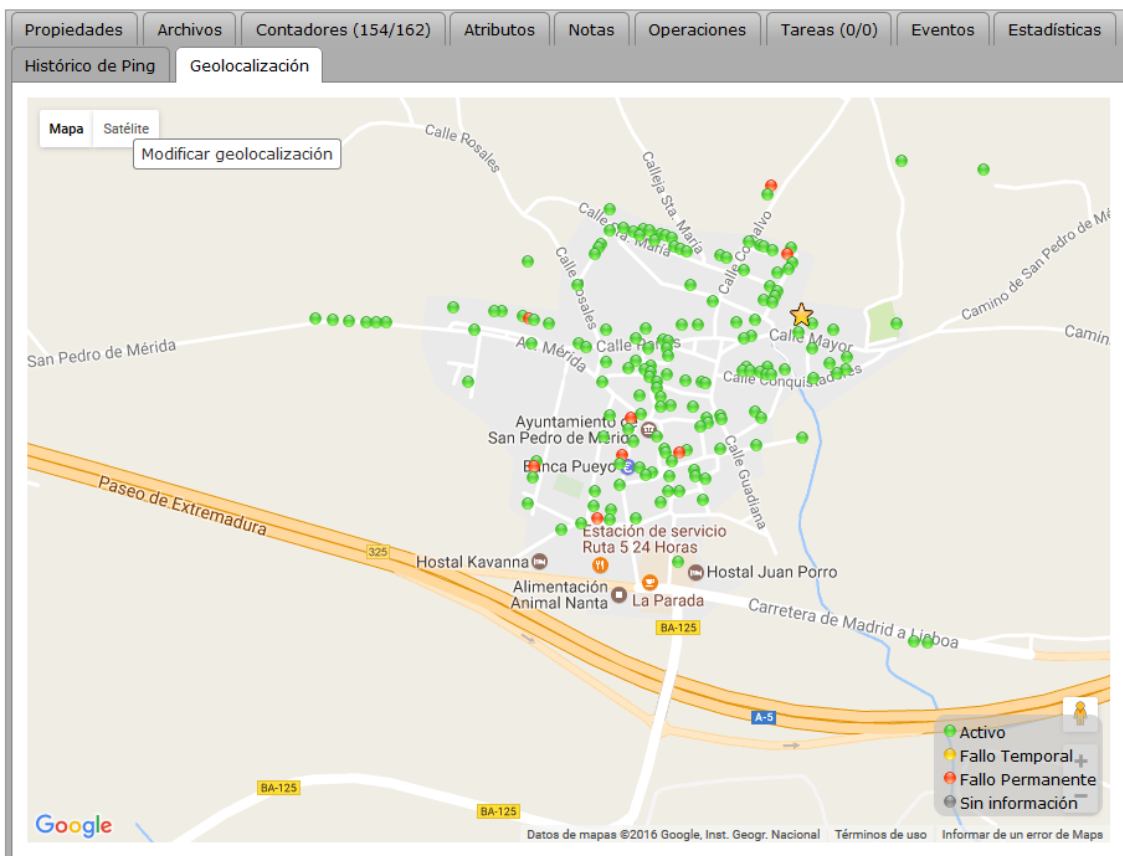


Figura 93 – Geolocalización del concentrador y sus contadores asociados

Capítulo 5

Impacto socio-económico

En este capítulo se presentan las implicaciones socio-económicas de este TFG. Se analiza el impacto de este proyecto teniendo en cuenta el contexto energético actual en España y se define la planificación seguida para su realización, así como el presupuesto del mismo

5.1 Impacto

Este Trabajo de Fin de Grado aborda lo que sin duda es un tema de actualidad con una gran relevancia para la inmensa mayoría de la población. Como ya se ha mencionado anteriormente, la legislación española establece que a partir del 31 de diciembre de 2018 todos los contadores del país deberán ser contadores inteligentes, con el necesario desarrollo de los diferentes sistemas MDM. Además, la proliferación de este tipo de tecnologías creará una fuerte demanda de profesionales cualificados, lo que se traduce en una importante próxima creación de empleo alrededor de los nuevos sistemas de medición inteligentes. En este sentido, el presente documento puede suponer una valiosa aportación debido a la finalidad fundamental con la que ha sido concebido, que no es otra que la de la formación de alumnos de grado o post-grado en el ámbito de las *Smart Grids*.

Por otro lado, el suministro energético no puede concebirse del mismo modo que se perciben otras actividades económicas cuyo objeto son bienes o servicios no imprescindibles, sino que está considerado como un derecho fundamental e imprescindible para el desarrollo de una vida digna. De este modo, la especulación comercial alrededor del suministro energético es una práctica que va contra los más principios éticos básicos e incluso contra la legalidad vigente. Por tanto, y como explica lo anteriormente expuesto, este TFG tiene profundas implicaciones sociales y debe ser visto como una herramienta para la comprensión de tecnologías que afectarán a la práctica totalidad de la sociedad.

5.2 Planificación

El presente Trabajo de Fin de Grado se ha desarrollado en cuatro fases: Análisis del Estado del Arte, Diseño, Ejecución y evaluación y Documentación.

Fase I: Análisis del Estado del Arte

Esta primera fase consistió en la realización de la investigación necesaria para conocer las tecnologías que entran en juego en este TFG, así como en la familiarización con el equipamiento de medida, IRIS, ZIV PRIME Manager y la Interfaz web del concentrador ZIV. Una vez realizadas estas tareas se consideró que existía una base suficiente para continuar con las siguientes fases del TFG. En total, esta primera fase conllevó 46 días de trabajo.

Fase II: Diseño

Durante esta fase se estudiaron los requisitos de diseño del manual de prácticas, se fijó su formato y se determinaron las cuestiones que mejor ayudarían a explorar el potencial de la infraestructura ciber-física para la telegestión de contadores inteligentes. Esta fase supuso un total de 18 días de trabajo.

Fase III: Ejecución y evaluación

Durante esta fase se ejecutaron las pruebas definidas en la Fase II y se documentó su resultado. Del mismo modo, se corrigieron y mejoraron ciertos aspectos del manual que con la ejecución se mostraron susceptibles de cambio o mejora y se solucionaron las dificultades técnicas que tuvieron lugar. Esta fase sirvió también a modo de aprendizaje ya que durante ella se despejaron numerosas dudas planteadas durante el estudio del estado del arte y el diseño del manual. Esta fase supuso un total de 24 días de trabajo.

Fase IV: Documentación

Durante esta fase se documentó la totalidad de este TFG con el objetivo de que este se ajustara a las directrices recomendadas para este tipo de trabajos. Para ello se necesitaron 36 días de trabajo.

5.3 Presupuesto

Para la realización de este TFG se ha utilizado el equipamiento proporcionado por el Departamento de Ingeniería Telemática.

- Portátil HP Pavilion G6
- Infraestructura ciber-física AMI
- Plataforma de telegestión IRIS
- ZIV PRIME Manager
- XML Translator
- OBIS Helper

Tanto la infraestructura ciber-física para la telegestión de contadores, como todo el software utilizado han sido proporcionados por los fabricantes en el marco del proyecto de investigación OSIRIS.

El ordenador portátil utilizado ha sido un HP Pavilion G6. Se establece que estos equipos tienen una vida útil de 48 meses. Según la tabla de coeficientes de amortización lineal elaborada por la Agencia Tributaria, los equipos para procesos de información (entre los que se incluyen los ordenadores) tienen un coeficiente de amortización anual de un 25% anual. Teniendo en cuenta que el ordenador solamente se ha utilizado durante 6 meses, el coeficiente de amortización será del 12,5%. En la siguiente tabla se muestra la amortización para el periodo durante el cual se ha utilizado este ordenador, es decir, 6 meses (desde finales de junio hasta finales de diciembre).

Concepto	Unidades	Coste/unidad	Amortización (%)	Total
Ordenador HP Pavilion G6	1	550 €	12,5	68,75 €

Tabla 12 – Costes materiales

Para calcular el coste en recursos humanos se tienen en cuenta las horas de trabajo, que son calculadas en base al tiempo dedicado por un ingeniero para llevar a cabo todas las fases del proyecto descritas en el **Apartado 5.2**. Desde el comienzo de este TFG hasta su finalización han transcurrido 6 meses, con un total de 119 días dedicados a su realización. Se asume una media de 4 horas por día trabajado, con lo que se obtienen un total de 496 horas trabajadas. El salario de un ingeniero junior se fija en 20 € por hora de trabajo.

Tarea	Días trabajados	Horas trabajadas	Coste/Hora (Ingeniero Junior)	Total
Análisis del Estado del Arte	46	184	20 €/hora	3.680 €
Diseño	18	72		1.440 €
Ejecución y Evaluación	24	96		1.920 €
Documentación	36	144		2.880 €
Total	125	496		9.920 €

Tabla 13 – Costes recursos humanos

El coste total del proyecto se calcula sumando los costes materiales y los costes en recursos humanos. A este coste final se le ha aplicado un impuesto de costes indirectos del 20%, como se indica en la Tabla 14.

Concepto	Total
Costes materiales	68,75 €
Costes recursos humanos	9.920 €
Coste total	9.988,75 €
Coste total (+20%)	11.986,50 €

Tabla 14 – Costes totales

Luego:

“El presupuesto total del proyecto asciende a la cantidad de **ONCE MIL NOVECIENTOS OCHENTA Y SEIS CON CINCUENTA** euros”

Leganés, febrero de 2017



Javier Olmeda Delgado

Capítulo 6

Conclusions and future works

In this last chapter of the TFG, the conclusions obtained after the completion of this project, as well as the knowledge acquired during its realization and future lines of research, are set out.

6.1 Conclusions

In this TFG, a practice manual has been developed, with its corresponding solutions, in which a battery of tests is defined with the goal of analyzing the potential of a cyber-physical infrastructure for Smart Meters remote management. This project has been raised and elaborated from an academic perspective for teaching use, so that the manual of practices elaborated in it can become part of future subjects to train professionals in the field of Smart Grids.

First, from a personal point of view, this TFG has allowed me to know in detail the current situation and future prospects of Smart Grids, and more specifically, of Advanced Metering Infrastructures, one of their fundamental components. Thanks to this project I have known in detail the current state of deployment of these metering systems, as well as the main regulatory and legislative aspects that affect such deployments.

Narrowband PLC (NB-PLC) technologies offer a series of advantages that are critical for DSOs. Firstly, the use of traditional electrical wiring for data transmission represents a radical reduction of infrastructure cost. In addition, the physical and capillarity characteristics of the power grid and the high performance of existing standards make PLC technology a good alternative. In the case of Smart Grids, NB-PLC technology is used, which ensures a greater range of action at the cost of a reduction in transmission speed, which does not harm the communication since this application does not require such high data rates.

In terms of communication protocols, the main standards involved in this TFG are related to the PRIME protocol stack. As an emerging but mature and consolidated in the market standard, as well as with great international projection for a promising future business such as Smart Grids, having learned its principles of operation and its application in communication between intelligent metering devices is a contribution of great value at professional level.

Also important is the acquisition of knowledge about DLMS/COSEM, the application layer protocol working on top of PRIME as well as on top of any other communications technology used for remote metering. After a previous phase of documentation, it has been possible to understand the different phases that take place in the communication between PRIME devices and the different types of existing messages. OBIS codes have made possible to identify different STG-DC reports requested to the meters. These reports are widely used in the professional environment of DSOs for obtaining information of the grid and change some of its parameters, so the familiarization with them means a better understanding of how DSOs manage the power grid.

Finally, the use of a commercial platform for remote management such as IRIS represents a contribution of huge value, since MDMS are of paramount importance in the future of energy sector. The definition of the new smart metering systems no longer covers only the meters, but also the remote management systems (Meter Data Management Systems), essential for network information processing and management. In this respect, this TFG has allowed me to remotely manage in an autonomous way a whole PRIME network through IRIS in a similar way as a DSO would, so my learning about the possibilities offered by these systems has been extensive. In addition, it is important to remark that, for the development of this project, I have worked in close collaboration with STM, which is another sign of real contact with industry.

The main goal of every TFG should be to bring the student closer to the job market, since it is the last step to complete university education and after that the student is supposed to be prepared to access the market and get a qualified job. In this regard, I consider that this TFG has clearly met this goal, since it has provided me with energy sector strongly linked knowledge, and with a direct application in it. In addition, the used tools, the learned technologies and protocols and the devices with which I have been able to work are a clear bet on the future in a constantly growing area such as Smart Grids. This TFG has therefore been a starting point in what can be a career in that field.

In addition, this TFG has also allowed me to get familiar with another side of university in that I have prepared a lab wording which can be incorporated (entirely or partly) into a subject in the future. This has allowed me to realize about the problematic of performing such a task and I have enjoyed it quite a lot at the same time.

6.2 Future Works

As a consequence of the realization of this TFG, I have been able to identify new lines of work that could prove useful in the future.

First, this TFG paves the road to continue analyzing the potential of the cyber-physical infrastructure and start to take advantage of some of its functionalities, since up to this point this infrastructure had not been fully exploited. This project will also facilitate the identification of deficiencies and points to improve in remote management and metering and may serve as a reflection to add new functionalities.

However, the main future work related to this TFG is its use for academic purposes. As it has been seen during its development, the base of this project is constituted by a lab manual with its corresponding solution. As an emerging and increasingly important field, it is expected that in the near future there will be a specific Master program for the study of Smart Grids. In this scenario, this TFG could be of great use as an aid to raise the lab of a subject of this Master.

Referencias

- [1] International Energy Agency, «Technology Roadmaps: Smart Grids», 2011.
- [2] G. López López, «Contribution to Machine-to-Machine Architectures for Smart Grids», Tesis Doctoral, Universidad Carlos III de Madrid, 2014.
- [3] EURELECTIRC, «Activity Report 2015», 2015.
- [4] Parlamento Europeo y Consejo de la Unión Europea, «Directiva 2009/72/CE del Parlamento Europeo y del Consejo, de 13 de junio de 2009, sobre normas comunes para el mercado interior de la electricidad y por el que se deroga la directiva 2003/54/CE», 2009.
- [5] «Real Decreto 1110/2007, de 24 de agosto, por el que se aprueba el Reglamento Unificado de Puntos de Medida del Sistema Eléctrico,» BOE, 2007.
- [6] «Orden ITC/3860/2007, de 28 de diciembre, por la que se revisan las tarifas eléctricas a partir del 1 de enero de 2008,» BOE, 2007.
- [7] G. López, J. I. Moreno, H. Amaris y F. Salazar, «Paving the road toward Smart Grid through Large-Scale Advanced Metering Infrastructures», *Electric Power Systems Research*, 2014. DOI: 10.1016/j.epsr.2014.05.006.
- [8] ITU-T standard G.9904, «Narrowband orthogonal frequency division multiplexing power line communication transceivers for PRIME networks», 2012.
- [9] «Página web oficial del proyecto OSIRIS,» [En línea]. Available: <http://www.unionfenosadistribucion.com/es/redes+inteligentes/investigacion+y+desarrollo>. [Último acceso: 20 12 2016].
- [10] FUNSEAM – Fundación para la Sostenibilidad Energética y Ambiental, «Informe Estratégico de la fundación para la sostenibilidad energética y ambiental», 2013.
- [11] N. Poveda, C. Medina y M. Zambrano, «Tecnologías de comunicación para redes de potencia inteligentes de media y alta tensión», Actualidad tecnológica, 2014.
- [12] A. Aidine, A. Tabone y J. Muller, «Deployment of Power Line Communication by European Utilities In Advanced Metering Infrastructure», IEEE ISPLC 2013, Johannesburg, South Africa, 2013.
- [13] ITU-T Standard G.9903, «Narrowband orthogonal frequency division multiplexing power line communication transceivers for G3-PLC networks», 2014.
- [14] «Página web oficial de la PRIME Alliance», [En línea]. Available: <http://www.prime-alliance.org/>. [Último acceso: 24 7 2016].
- [15] A. Martínez Sánchez, «Desarrollo de un módulo de análisis de mapas Shapefile para un simulador de redes PRIME,» Proyecto Fin de Carrera, Leganés, 2016.
- [16] A. J. Ferré Collado, «Aplicación WEB para automatización y visualización de simulaciones de redes PRIME,» Proyecto Fin de Carrera, Leganés, 2015.
- [17] DLMS User Association, «DLMS/COSEM Architecture and Protocols, Sixth Edition», 2007.

- [18] Fraunhofer Institute for Solar Energy Systems ISE, «jDLMS User Guide», 2016.
- [19] DLMS User Association, «COSEM Identification System and Interface Objects, Fourth Edition», 2001.
- [20] DLMS User Association, «DLMS/COSEM Architecture and Protocols, Ed. 8», 2014.
- [21] IEC 62056-53 International Standard, «Electricity metering - Data exchange for meter reading, tariff and load control - Part 53: COSEM application layer», 2002.
- [22] The UPGRID Consortium, «Scope and Boundaries of Project Demonstrations - Report on Standards and potential synergies», 2015.
- [23] Z. Sumic, «Gartner Report: Magic Quadrant for Meter Data Management Products », 2015.
- [24] Telecontrol STM Factoría Software, «Manual de usuario para la Plataforma de Telegestión IRIS v0.7.3», 2014.
- [25] «Página web oficial de Telecontrol STM» [En línea]. Available: <http://www.telecontrolstm.com/es/iris-software-platform>. [Último acceso: 19 12 2016].
- [26] «Página web oficial icube» [En línea]. Available: http://www.icube.ch/xmltranslator/xml_translator.html. [Último acceso: 16 12 2016].
- [27] «Página web oficial icube» [En línea]. Available: <http://www.icube.ch/obishelper/obishelper.html>. [Último acceso: 16 12 2016].
- [28] Parlamento Europeo y Consejo de la Unión Europea, «Directiva 2004/22/CE del Parlamento Europeo y del Consejo, de 31 de marzo de 2004, relativa a los instrumentos de medida», 2004.
- [29] Comisión Europea «M/374 Mandate to CEN and CENELEC for standardisation in the field of measuring instruments», 2005.
- [30] Parlamento Europeo y Consejo de la Unión Europea «Directiva 2006/32/CE del Parlamento Europeo y del Consejo, de 5 de abril de 2006, sobre la eficiencia del uso final de la energía y los servicios energéticos y por la que se deroga la Directiva 93/76/CEE del consejo», 2006.
- [31] F. J. Leiva Rojo, «Análisis regulatorio, técnico y económico de los sistemas de medida inteligente,» Trabajo de Fin de Máster, Escuela Técnica Superior de Ingeniería, Universidad de Sevilla, 2013.
- [32] Parlamento Europeo y Consejo de la Unión Europea, «Directiva 2012/27/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, relativa a la eficiencia energética, por la que se modifican las directivas 2009/125/CE y 2010/30/UE, y por la que se derogan las Directivas 2004/8/CE y 2006/32/CE», 2012.
- [33] Comisión Europea, «Recomendación de la Comisión, de 9 de marzo de 2012, relativa a los preparativos para el despliegue de los sistemas de contador inteligente», 2012.
- [34] «Orden ITC/3022/2007, de 10 de octubre, por la que se regula el control metrológico del Estado sobre los contadores de energía eléctrica, estáticos combinados, activa, clases A,B y C y reactiva, clases 2 y 3, a instalar en suministros de energía eléctrica hasta una potencia de 15 kW de activa que incorporan dispositivos de discriminación horaria y telegestión, en las fases de evaluación de la conformidad,

verificación después de reparación o modificación y de verificación periódica», BOE, 2007.

[35] «Orden IET/290/2012, de 16 de febrero, por la que se modifica la Orden ITC/3860/2007, de 28 de diciembre, por la que se revisan las tarifas eléctricas a partir del 1 de enero de 2008 en lo relativo al plan de sustitución de contadores», BOE, 2012.

ANNEX I

Extended Abstract

1. Motivation

In an increasingly complex and interconnected society, it is difficult to think of a sector in which Information and Communication Technologies (ICT) are not present, and the energy sector is no exception. ICT development is being key for this sector, which seeks to respond to the new needs of customers by promoting a more flexible and efficient management of networks through the so-called Smart Grids. Smart Grids are those ones which are capable of integrating the behavior and actions of all customers connected to it in an agile and efficient way, including a wide variety of operational and energy measures and ensuring a more sustainable and efficient power grid with low losses and high quality and safety levels [1].

Smart Grids represent a real revolution, since they are systems that allow bidirectional communication between the customer and the public utility company, so that the latter can store the information provided by the former in order to improve the management of its network. In addition, with the growing presence of renewable energies we face the scenario that the customer is not only an energy consumer, but also a producer. It is therefore important that this networks facilitate the progressive incorporation of such renewable energies taking into account their particularities and limitations.

The M2M (Machine-to-Machine) communications concept, which refers to data exchange between two remote machines, is particularly important in Smart Grids, since they allow the bidirectional exchange of information in real time between the managed and monitored devices and the data storage and processing systems. Among the devices that use M2M communications stand out the AMI (Advanced Metering Infrastructure), including smart meters which communicate with public utility systems. On the other hand, the recent advances in data processing and management, with the emerging big data leading the way, are particularly relevant since they will make it possible to manage and process data in order to make decisions based on this large amount of information [2].

According to the annual report of 2015 conducted by EURELECTRIC [3], the sector association which represents the common interests of the electricity industry at a European level, electricity companies throughout next ten years are expected to invest 350 billion euros in the deployment of Smart Grids for around 260 million customers. The European Directive 2009/72/EC [4] included means to protect consumers, including the obligation of Member States to ensure the use of smart meters.

In Spain, the progressive implementation of this type of meters has been planned since 2007. In this year, the Royal Decree 1110/2007 [5], which establishes the necessary functionalities of remote management systems and also the requirements to be met by metering equipment, was approved, and the Order ITC/3860/2007 [6] which details the “Meter replacement plan” and establishes the deadline for its total implementation in Spain on December 31, 2018.

Among the different methods that can be considered for the transmission of information in Smart Grids, PLC (Power Line Communications) technology is very interesting for direct communication with Smart Meters in the so-called last mile of the Advanced Metering Infrastructures due to the use of existing electric infrastructure (electrical wiring) as a communication medium. The use of PLC technology is particularly interesting for the electrical distributors (DSO or Distribution System Operator), since it does not require the deployment of new infrastructures for communications. Because power cables are not intended to be used as a communication medium, they offer a rather hostile environment from the point of view of data transmission, due to factors such as noise or impedance variation. Despite this, PLC offer many valuable advantages to DSOs, especially Narrowband PLS (NB-PLC), whose standards were developed to mitigate some of the problems in PLC communications. Currently, these NB-PLC standards are being widely used for communication between Smart Meters and data concentrators in AMI deployments [7].

At present, there are different NB-PLC standards, being PRIME (PowerLine Intelligent Metering Evolution) and Meters & More the most widely used in Spain. PRIME technology, as mentioned, is widely deployed in Spain and represents a mature standard with international projection and used by some of the largest DSOs in Spain like Iberdrola and Fenosa.

PRIME standard is promoted by the PRIME Alliance, led by Iberdrola, and is a free, open and not subject to intellectual property rights. Due to this fact, it makes it easy that new entrants can provide interoperable solutions. Its aim is to provide a standard among equipment and systems from different vendors [8].

Along with PRIME, new communication protocols are designed to enable the transmission of information between different elements of Smart Grids. One of these protocols is DLMS/COSEM (IEC 62056), application layer protocol designed specifically for communication with Smart Meters. DLMS (Distribution Line Message Specification) is the PRIME application layer protocol and supports functions such as

remote meter reading, remote control and value-added services to measure any type of energy. COSEM (Companion Specification for Energy Metering) is the data model used for communication between measuring equipment.

Smart Grids deployment also has one of its main attractions in the possibility that DSOs can remotely manage their power grid. Due to this fact, different platforms and Smart Grids remote management systems that provide the necessary functionalities for grid management have emerged, as well as a wide range of statistics to know in detail the state of the different elements of the grid in real time. STG-DC protocol, based on web services, is defined for the communication between these remote management platforms (STG or *Sistema de TeleGestión*) and the data concentrators (DC). The PRIME meters and concentrators remote management platform to be used and analyzed in this TFG is IRIS, intended for commercial use and developed by STM Telecontrol.

The research group of the Telematics Engineering Department in which this TFG has been developed is framed within the OSIRIS project (*Optimización de la Supervisión Inteligente de la Red de Distribución*) [9], financed by the Ministry of Economy and Competitiveness and led by Union Fenosa Distribución (third national electricity distributor). For this research group a cyber-physical infrastructure fully manageable from IRIS is available. This infrastructure is composed of both physical and virtual devices. In the physical part, there are four smart meters, all of them of ZIV brand, associated to a data concentrator also from ZIV. The virtual part of the infrastructure is larger and can give an idea of the number of devices that a DSO may have to remotely manage. This virtual infrastructure consists of ten concentrators, each with a number of associated meters ranging from 150 to 170.

Because both the concept of Smart Grid and the different technologies involved in its deployment are relatively recent, the training of qualified professionals in this field is still at an early stage, both at the corporate and academic levels. However, the energy sector revolution brought about by the development of Smart Grids and the prospects for the future that are envisaged around them are leading to a growing demand for this type of professionals.

Motivated by these growing needs in the field of Smart Grids, this TFG arises with the purpose of bringing the student closer to these ever more present future networks. It will deal with aspects of different segments of a Smart Grid, from the communication between devices to its remote management through IRIS, in order to analyze the potential of the available cyber-physical infrastructure.

2. Goals

The main goal of this TFG is to develop a battery of tests that illustrates the functionality and potential of the available cyber-physical infrastructure. This set of tests will be raised from a teaching point of view, for its use in the academic field. Therefore, this practice manual can be used in future subjects in order to train professionals in the competences related to the field of Smart Grids.

In order to reach this final goal, a series of intermediate steps or sub-goals which will guide this TFG have been defined:

- Analysis of the state of the art of the different technologies involved in PRIME networks and that are relevant to this TFG.
- Documentation of the use of the different tools that need to be used to achieve the main objective.
- Elaboration of a practice manual with a set of tests that allow a thorough analysis of the available cyber-physical infrastructure potential and functionality.
- Elaboration of a solution of the mentioned practice manual that include each individual solution and in which the methodology to follow to carry out each single test is defined, as well as the analysis of the obtained results, including the corresponding illustrative material.
- Accurate documentation of all the process carried out.

3. Memory structure

This TFG is intended to serve as a guide for potential labs, so it includes all the necessary information for this purpose, from the summaries of the communication protocols to the manuals of the involved tools. It is essential to provide future users with all the necessary information to prepare a lab manual aimed to be a part of the course syllabus so that this manual can be as complete as possible. This explains the final length of the memory, which is significantly higher than the recommended one. However, the main contribution of this TFG is the definition of the battery of tests along with its corresponding solution (Chapters 3 and 4). The rest of the sections can be consulted by the reader to allow him to expand knowledge or understand other parts of the project.

This TFG is organized in different chapters that cover each of the phases of its realization. The structure and content are detailed below:

- **Chapter 1: Introduction**

This chapter provides an overview of the TFG, including an introduction to the PLC communication technology, focusing on PRIME standard. It sets out the reasons that have led to the realization of this TFG, the objectives to be achieved with it and the structure of this document.

- **Chapter 2: State of the art**

This chapter analyzes the state of the art of the different technologies related to this TFG and that take part in the deployment of AMI, focusing mainly on PRIME and other related protocols, and on the tools used during the development of this project. In addition, the cyber-physical infrastructure is presented in detail. Finally, the regulatory framework applicable at both national and European level is set out.

- **Chapter 3: Design**

This chapter describes the requirements and restrictions for the preparation of the lab manual. After defining these points, the manual, composed by the battery of tests to be carried out on the cyber-physical infrastructure, is presented. The tests are designed to make use of the tools described in **Chapter 2** and to test the knowledge about the involved technologies with the ultimate goal of illustrating and analyzing the potential of the cyber-physical infrastructure.

- **Chapter 4: Results and evaluation**

This chapter details the results of the different tests carried out on the cyber-physical infrastructure, in order to give a clear view about its potential. For this purpose, each test result is analyzed in a clear and illustrative way.

- **Chapter 5: Socio-economic impact**

In this chapter, the socio-economic implications of this TFG are presented. It analyses the impact of this project taking into account the current energetic context in Spain and presents the planning followed for its realization along with its budget.

- **Chapter 6: Conclusions**

In this last chapter of the TFG, the conclusions obtained after the completion of this project, as well as the knowledge acquired during its realization and future lines of research, are set out.

- **ANNEXES**

- **Annex 1:** Extended Abstract
- **Annex 2:** STG-DC reports and orders.
- **Annex 3:** IRIS user manual.

- **Annex 4:** ZIV PRIME Manager user manual.
- **Annex 5:** ZIV Concentrator web interface user manual

4. Conclusions

In this TFG, a practice manual has been developed, with its corresponding solutions, in which a battery of tests is defined with the goal of analyzing the potential of a cyber-physical infrastructure for Smart Meters remote management. This project has been raised and elaborated from an academic perspective for teaching use, so that the manual of practices elaborated in it can become part of future subjects to train professionals in the field of Smart Grids.

First, from a personal point of view, this TFG has allowed me to know in detail the current situation and future prospects of Smart Grids, and more specifically, of Advanced Metering Infrastructures, one of their fundamental components. Thanks to this project I have known in detail the current state of deployment of these metering systems, as well as the main regulatory and legislative aspects that affect such deployments.

Narrowband PLC (NB-PLC) technologies offer a series of advantages that are critical for DSOs. Firstly, the use of traditional electrical wiring for data transmission represents a radical reduction of infrastructure cost. In addition, the physical and capillarity characteristics of the power grid and the high performance of existing standards make PLC technology a good alternative. In the case of Smart Grids, NB-PLC technology is used, which ensures a greater range of action at the cost of a reduction in transmission speed, which does not harm the communication since this application does not require such high data rates.

In terms of communication protocols, the main standards involved in this TFG are related to the PRIME protocol stack. As an emerging but mature and consolidated in the market standard, as well as with great international projection for a promising future business such as Smart Grids, having learned its principles of operation and its application in communication between intelligent metering devices is a contribution of great value at professional level.

Also important is the acquisition of knowledge about DLMS/COSEM, the application layer protocol working on top of PRIME as well as on top of any other communications technology used for remote metering. After a previous phase of documentation, it has been possible to understand the different phases that take place in the communication between PRIME devices and the different types of existing messages. OBIS codes have made possible to identify different STG-DC reports requested to the meters. These reports are widely used in the professional environment of DSOs for obtaining information of the grid and change some of its parameters, so the

familiarization with them means a better understanding of how DSOs manage the power grid.

Finally, the use of a commercial platform for remote management such as IRIS represents a contribution of huge value, since MDMS are of paramount importance in the future of energy sector. The definition of the new smart metering systems no longer covers only the meters, but also the remote management systems (Meter Data Management Systems), essential for network information processing and management. In this respect, this TFG has allowed me to remotely manage in an autonomous way a whole PRIME network through IRIS in a similar way as a DSO would, so my learning about the possibilities offered by these systems has been extensive. In addition, it is important to remark that, for the development of this project, I have worked in close collaboration with STM, which is another sign of real contact with industry.

The main goal of every TFG should be to bring the student closer to the job market, since it is the last step to complete university education and after that the student is supposed to be prepared to access the market and get a qualified job. In this regard, I consider that this TFG has clearly met this goal, since it has provided me with energy sector strongly linked knowledge, and with a direct application in it. In addition, the used tools, the learned technologies and protocols and the devices with which I have been able to work are a clear bet on the future in a constantly growing area such as Smart Grids. This TFG has therefore been a starting point in what can be a career in that field.

In addition, this TFG has also allowed me to get familiar with another side of university in that I have prepared a lab wording which can be incorporated (entirely or partly) into a subject in the future. This has allowed me to realize about the problematic of performing such a task and I have enjoyed it quite a lot at the same time.

5. Future Works

As a consequence of the realization of this TFG, I have been able to identify new lines of work that could prove useful in the future.

First, this TFG paves the road to continue analyzing the potential of the cyber-physical infrastructure and start to take advantage of some of its functionalities, since up to this point this infrastructure had not been fully exploited. This project will also facilitate the identification of deficiencies and points to improve in remote management and metering and may serve as a reflection to add new functionalities.

However, the main future work related to this TFG is its use for academic purposes. As it has been seen during its development, the base of this project is constituted by a lab manual with its corresponding solution. As an emerging and

increasingly important field, it is expected that in the near future there will be a specific Master program for the study of Smart Grids. In this scenario, this TFG could be of great use as an aid to raise the lab of a subject of this Master.

ANEXO II

Informes y órdenes STG-DC

	ID	Contenido	P ¹	A/S ²	FTP/WS	WS Serv./Nombre	TP ³	Ámbito	Comentarios
Órdenes	B02	Modificación de potencia contratada	1	A	WS	DC-Order	No	1 Cont.	
	B03	Desconexión / Reconexión	1	A	WS	DC-Order	No	1 Cont.	
	B04	Modificaciones contractuales	1	A	WS	DC-Order	No	1 Cont.	
	B05	Actualización <i>firmware</i> Contadores	1	A	WS	DC-Order	No	1/N Cont.	Unicast/multicast/broadcast PRIME/DLMS
	B06	Eliminar Contador	3	A	WS	DC-Order	No	1 Cont.	
	B07	Modificación configuración CNTR	2	A	WS	DC-Order	No	1 Cont.	
	B08	Actualización <i>firmware</i> CNTR	1	A	WS	DC-Order	No	1/N CNTR	Unicast/multicast/broadcast
	B09	Modificación configuración Contador	2	A	WS	DC-Order	No	1 Cont.	
	B11	Solicitud de orden DC	2	A	WS	DC-Order	No	1 Cont.	
Informes	S01	Valores instantáneos Contadores	3	S	WS	DC-Request STG-Report	No	1 Cont.	
	S02	Perfil de carga (diario incremental)	1	A	FTP	STG-URS	Sí	CT	
	S03	Perfil de carga (diario absoluto)	2	A	FTP	STG-URS	Sí	CT	
	S04	Facturación mensual	1	A	FTP	STG-URS	Sí	CT	
	S05	Facturación diaria	1	A	FTP	STG-URS	Sí	CT	
	S06	Parámetros Contadores	3	A	FTP	STG-URS	Sí	CT	
	S07	Fallo de voltaje	3	A	FTP	STG-URS	Sí	CT	

¹ P=Prioridad. 1 =Actualmente en uso; 2 = Corto plazo; 3 = Largo plazo/puede no llegar a implementarse.

² A= Asíncrono; S = Síncrono.

³ TP = Tarea Programable

S08	Calidad de potencia (PQ)	3	A	FTP	STG-URS	Sí	CT	
S09	Eventos Contadores	2	A	FTP	STG-URS	Sí	CT	
S10	Equipo intruso en PLC	3	A	FTP	STG-URS	Sí	CT	
S11	Información Nodo Base (CNTR)	1	A	FTP	STG-URS	Sí	CT	
S12	Parámetros CNTR	2	A	FTP	STG-URS	Sí	CT	
S13	Evento espontáneo Contador	2	A	WS	STG-Report	No	1 Cont.	
S14	Perfil de voltaje y corriente	3	A	WS	STG-Report	No	1 Cont.	
S15	Evento espontáneo CNTR	2	A	WS	STG-Report	No	1 Cont.	
S17	Evento CNTR	2	A	FTP	STG-URS	Sí	CT	
S18	Confirmación de desconexión	3	A	WS	STG-Report	No	1 Cont.	
S19	Confirmación actualización <i>firmware</i> Contador	3	A	WS	STG-URS	No	1/N Cont.	Unicast/multicast/broadcast PRIME/DLMS
S20	Lista de Contadores controlados	2	A	FTP	STG-URS	Sí	CT	
S21	Valores instantáneos avanzados	3	S	WS	DC-Request	No	1 Cont.	
S22	Confirmación actualización <i>firmware</i> CNTR	3	A	WS	STG-URS	No	1/N CNTR.	Unicast/multicast/broadcast
S23	Definición de contrato	1	A	FTP	STG-URS	Sí	CT	
S24	Tabla de Contadores presentes en red PRIME	3	A	FTP	STG-URS	Sí	CT	
S26	Valores instantáneos bajo demanda	3	A	FTP	STG-URS	Sí	CT	
S27	Valores de facturación actuales bajo demanda	2	S	WS	STG-Report	No	1 Cont.	
G01	Estadísticas horarias de comunicación con Contadores	2		FTP	STG-URS	Sí	CT	
G02	Estadísticas diarias de comunicación con Contadores	2		FTP	STG-URS	Sí	CT	
G03	Curva media (MED) de V, I y P	1		FTP	STG-URS	Sí	1 Cont.	
G04	Curva máxima (MAX) de V, I y P	1		FTP	STG-URS	Sí	1 Cont.	
G05	Curva mínima (MIN) de V, I y P	2		FTP	STG-URS	Sí	1 Cont.	
G06	Curva instantánea (MOM) de V, I y P	3		FTP	STG-URS	Sí	1 Cont.	
G07	Curva media (MED) de desbalances y armónicos	3		FTP	STG-URS	Sí	1 Cont.	
G08	Parámetros extendidos de	2		FTP	STG-URS	Sí	1 Cont.	

		Contadores							
	G09	Parámetros de I/O digitales	1		FTP	STG-URS	Sí	1 Cont.	
Gestión		Sincronización (NTP)	1						
		Monitorización	3						
		Señalización	3						
		Acceso remoto CNTR	2						
		Alarmas CNTR	3						
		Tráfico 104	1						

ANEXO III

Manual de usuario de IRIS

1. Introducción

El siguiente manual es un resumen del manual oficial de IRIS proporcionado por Telecontrol STM [24].

IRIS es la Plataforma abierta de telegestión de concentradores y contadores PRIME desarrollada por Telecontrol STM. Una de las mayores ventajas que tienen los contadores inteligentes con respecto a los tradicionales es la de la posibilidad de realizar su gestión y mantenimiento a distancia, sin la necesidad de que un técnico acuda de forma física al lugar de la ubicación del contador. Por tanto, IRIS es una plataforma que nos va a permitir sacar todo el partido a las nuevas redes inteligentes basadas en PRIME.

El apartado Gestión de Dispositivos del portal de IRIS es el que nos permitirá consultar todas las estadísticas relativas a nuestra red, tanto física como virtual, así como modificar y configurar las características de la red de contadores. Al acceder a dicho apartado se nos mostrará el panel de control. En la vista “Estado de ping y PLC” podremos ver las estadísticas de ping, realizadas tanto a los concentradores como a los contadores, de modo que tendremos una vista simple y general del funcionamiento de los dispositivos. La vista “Listado de estadísticas” permite ver de manera resumida las estadísticas básicas del sistema. Por último, “Estadísticas de tareas” refleja la información relativa a las conexiones, desconexiones y cambios en la potencia máxima llevadas a cabo en el sistema, ya sea por días del mes o por meses completos.

2. Concentradores

En el desplegable “Concentradores” podemos ver diferentes pantallas en las que se nos muestran los concentradores del sistema de acuerdo a la característica seleccionada.

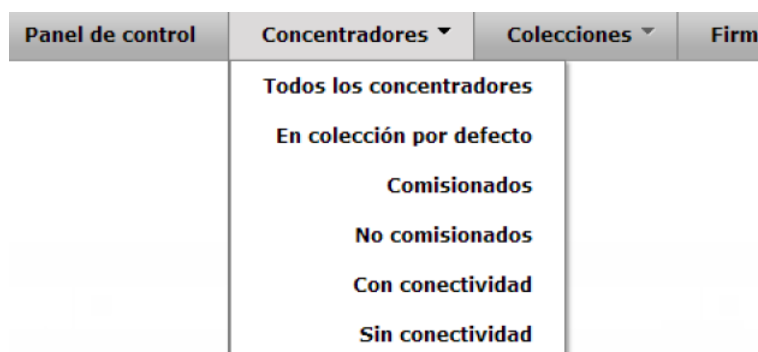


Figura 94 – Pestaña “Concentradores”

Los concentradores del sistema se muestran ordenados por número de serie. Para añadir nuevos concentradores solamente habrá que seleccionar la opción “Añadir Concentrador”, siendo necesario introducir su URL/IP y número de serie únicamente, aunque seleccionando opciones avanzadas aparecerá un formulario más completo. Podemos añadir este nuevo contador a una colección, ya sea una que exista previamente o una creada en ese mismo momento.

En adelante, este símbolo indicará la posibilidad de exportar la opción actual en una hoja de Excel.



2.1 Acciones de concentrador

Sobre los diferentes concentradores es posible realizar un amplio número de acciones. Para ello se debe seleccionar uno o varios concentradores y hacer clic sobre “Acciones”.

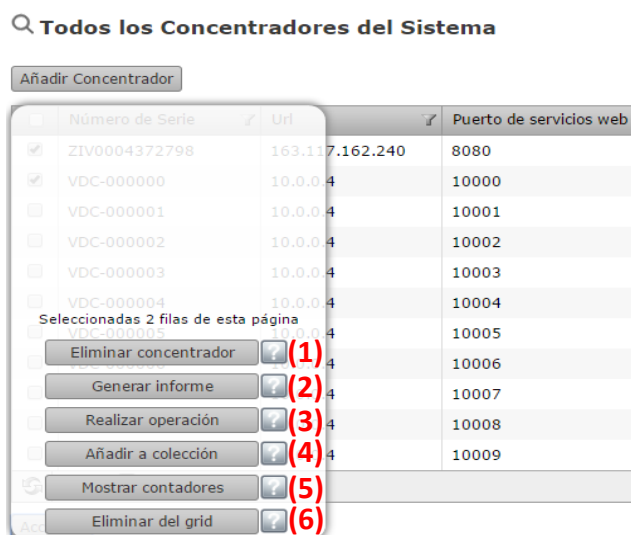


Figura 95 – Acciones de concentrador

En el desplegable tenemos una lista de las acciones que es posible realizar en el concentrador. La acción **“Eliminar concentrador”** (1) elimina el concentrador o concentradores seleccionados del sistema, mientras que la acción **“Eliminar del grid”** (6) lo que hace es eliminar estos contadores con los que ya no quiero trabajar de la lista de trabajo, no del sistema IRIS. Es posible también añadir la selección a una colección ya existente mediante la acción **“Añadir a colección”** (4). Seleccionando **“Mostrar contadores”** (5) se muestra una lista con todos los contadores asociados a los contadores seleccionados.

Mediante la acción **“Generar informe”** (2) tenemos la posibilidad de seleccionar la cantidad de información que incluirá el informe, aunque disponemos de una serie de plantillas para realizar informes en las que no sería necesario seleccionar esta información, puesto que viene prefijada. También es posible guardar informes personalizados para crear nuevos tipos o plantillas.

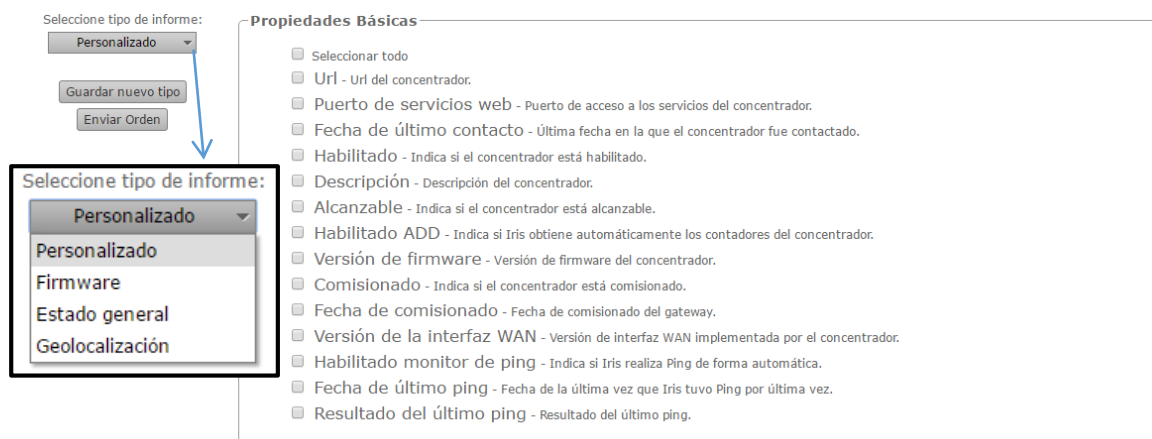


Figura 96 – Informes de concentrador

Seleccionando “Realizar operación” (3) se mostrarán una serie de operaciones entre las cuales elegiremos la que queremos lanzar en los concentradores seleccionados. Las operaciones que podemos realizar son las que se pueden ver en la siguiente imagen.

Operaciones de concentrador

The interface displays a list of selected concentrators on the left and four panels of operations on the right:

- Concentradores seleccionados:**
 - ZIV0004372798
 - VDC-000000
- Órdenes:**
 - Descubrimiento Automático de Contadores
 - Actualización de Firmware (B08)
 - Solicitud de orden (B11)
- Peticiones:**
 - Información de Nodo Base PLC (S11)
 - Parámetros del Concentrador (S12)
 - Eventos de Concentrador (S17)
 - Lista de Contadores Registrados (S20)
 - Lista de Contadores en la red PLC (S24)
- Informes:**
 - Informe del Balance del Concentrador
 - Informe de Comportamiento Inadecuado
 - Informe de Estado Actual PLC
- Peticiones avanzadas:**
 - Resumen horario PLC (G01)
 - Resumen diario PLC (G02)
 - Curva media avanzada (G03)
 - Curva máxima avanzada (G04)
 - Curva mínima avanzada (G05)
 - Curva instantánea avanzada (G06)
 - Armónicos - Curva media (G07)
 - Parámetros extendidos de contador (G08)
 - Parámetros de I/O digital (G09)
 - Trabajos en curso (G10)
 - Registro de peticiones y tareas (G11)
 - Rendimiento del concentrador (G12)
 - Ficheros transmitidos por FTP (G13)
 - Actualizaciones de firmware (G14)

Figura 97 – Operaciones de concentrador

Las operaciones se dividen en órdenes, peticiones, informes y peticiones avanzadas. Desde aquí existen múltiples posibilidades, como ordenar una actualización de firmware (B08) del concentrador o grupo de concentradores, solicitar la información del nodo base (S11) para visualizar por ejemplo sus nodos de servicio registrados, solicitar al concentrador la lista de contadores registrados en él (S20) u obtener el resumen horario y diario PLC (G01 y G02) para conocer el tiempo durante el que ha funcionado cada concentrador. Cabe destacar la petición S24 (lista de contadores en red PLC), ya que en ella se basa el comisionado de los concentradores.

2.2 Administrar la red de dispositivos del concentrador

En la vista de todos los concentradores también existe la opción de editar las propiedades básicas de un concentrador, para ello sólo hay que hacer clic sobre el concentrador en cuestión. En la nueva vista que se abre tenemos diferentes pestañas.

2.2.1 Propiedades

En esta pestaña podemos ver la información básica del concentrador. Dicha información puede ser modificable o no modificable (con carácter informativo).

☆ Número de Serie del Concentrador: **ZIV0004372798**

Propiedad	Valor	Estado
Url	163.117.162.240	
Puerto de servicios web	8080	
Descripción	UC3M	
Habilitado		<input checked="" type="checkbox"/>
Alcanzable		<input checked="" type="checkbox"/>
Habilitado ADD		<input checked="" type="checkbox"/>
Habilitado monitor de ping		<input checked="" type="checkbox"/>
Versión de firmware	4WF01611001_RC5b	
Versión de la interfaz WAN	3.1.c	
Comisionado		<input checked="" type="checkbox"/>
Fecha de comisionado	26/06/2015 09:56:09	
Fecha de último contacto	01/04/2016 08:00:17	
Fecha de último ping	01/04/2016 08:00:47	
Resultado del último ping		<input checked="" type="checkbox"/>

Eliminar concentrador

Mostrar colecciones

Añadir a colección

Figura 98 – Propiedades del concentrador

Entre la información mostrada está la información de comisionado, en la que se indica si el concentrador está comisionado y la fecha de dicho comisionado. Cuando se añade manual o automáticamente un concentrador, éste lanza lo que se denomina la *tarea de comisionado*, mediante la cual IRIS realiza las siguientes operaciones:

- Comprueba que existe conectividad con el concentrador.
- Cuando IRIS certifica que existe conectividad con el concentrador, averigua su versión WAN, que puede ser la 3.0 o la 3.1 o 3.1c. IRIS necesita conocer la versión WAN para saber cómo tiene que comunicar con el concentrador.
- Una vez que CONOCE LA VERSIÓN WAN, IRIS le solicita la lista actual de contadores al concentrador (a través del informe S24) y registra automáticamente esos contadores en IRIS.

2.2.2 Archivos

En “Archivos” es donde se encuentran todos los archivos generados por el concentrador y donde estos pueden ser inspeccionados.

2.2.3 Contadores

La pestaña de “Contadores” es a través de la cual podemos acceder a todos los contadores asociados al concentrador seleccionado y desde donde podremos llevar a

cabo la gestión de estos. Por ser posiblemente la pestaña que más nos interesa, será explicada en detalle más adelante.

2.2.4 Atributos

IRIS define dos tipos de atributos: atributos “Sistema”, propios de los dispositivos y que sólo pueden ser modificados con los permisos adecuados, y atributos “Libres”, que se pueden añadir libremente a los dispositivos desde cero para la comodidad del usuario de la plataforma, así como ser eliminados y modificados sin ninguna restricción (por ejemplo, identificadores particulares de la compañía eléctrica, atributos de geolocalización, identificadores de clientes, etc.).

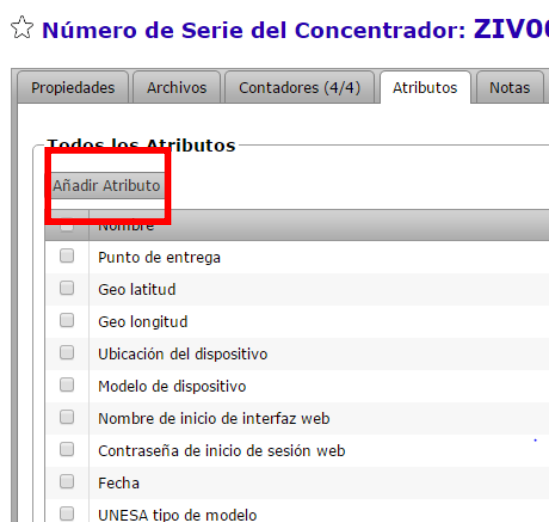


Figura 99 – Añadir atributo a un concentrador

Para añadir un atributo libre, simplemente hay que seleccionar “Añadir Atributo” e introducir su nombre y su valor. De manera opcional podremos marcar el atributo como relevante, de manera que aparecerá en una tabla de “Atributos Relevantes” situada en la parte superior de la pantalla (justo encima de la tabla “Todos los atributos”).

Figura 100 – Añadir atributo libre

2.2.5 Notas

IRIS permite asociar notas a cualquier dispositivo con la información que el usuario considere oportuna.

2.2.6 Operaciones

Para ejecutar operaciones en el concentrador, este debe encontrarse habilitado y alcanzable, así como estar comisionado. Las distintas operaciones se dividen en órdenes, peticiones, informes, eventos y peticiones avanzadas. Esta opción es similar a la de “Operaciones de concentrador” que se ha visto anteriormente, con la salvedad de que en esta ocasión solo se pueden ejecutar sobre un concentrador, mientras que en la vista de todos los concentradores podemos seleccionar varios para ejecutar operaciones sobre ellos.



Figura 101 – Operaciones del concentrador seleccionado

2.2.7 Tareas

El hecho de lanzar una operación conlleva la ejecución de la tarea que tiene asociada. En el momento en el que se lance esta operación el IRIS nos redirigirá de manera automática a la pestaña “Tareas”. En ella se mostrará el estado de todas las

operaciones que hayamos lanzado en el concentrador, indicando si la tarea está en curso o se ha finalizado y, en caso de haber finalizado, si ha sido exitosa o, por el contrario, se ha producido algún fallo en su ejecución. Las tareas en curso pueden ser interrumpidas en cualquier momento por el usuario. Cuando una tarea finaliza de forma exitosa es posible ver su resultado haciendo clic sobre dicha tarea.

2.2.8 Eventos

Esta pestaña permite visualizar todos los eventos que han tenido lugar en el concentrador. Uno de los eventos más importantes es el evento de fraude, el cual notifica a la distribuidora que se está produciendo un uso fraudulento de la red. Este evento se basa en las medidas tomadas por el llamado contador supervisor, que es un contador que toma medidas del consumo de toda la subred (a menudo se encuentra dentro del propio concentrador). Este contador, por tanto, mide la suma de los consumos de todos los contadores de la subred, teniendo en cuenta que siempre será ligeramente superior a la suma real debido a las pérdidas. Cuando el consumo medido por el supervisor no coincide con la suma de los valores medidos por los contadores, teniendo en cuenta las mencionadas pérdidas, tendría lugar el evento de fraude.

2.2.9 Estadísticas

Esta pestaña muestra la información relativa al concentrador.

Propiedades	Archivos	Contadores (154/162)	Atributos	Notas	Operaciones	Tareas (0/0)	Eventos
Estadísticas	Histórico de Ping	Geolocalización					

Nombre de la Estadística	Valor de la Estadística	Fecha
Número de contadores por concentrador	162	19/12/2016 12:02:51
Nº de contadores activos por concentrador	154	19/12/2016 12:02:52
Nº de contadores con fallo temporal por concentrador	0	19/12/2016 12:02:52
Nº de contadores inactivos por concentrador	8	19/12/2016 12:02:51
Ping con éxito en los últimos 7 días %	100%	19/12/2016 12:00:15
Nº de archivos del último día por gateway	22	19/12/2016 12:00:30
Cierre diario % por concentrador	100%	19/12/2016 12:00:29
Cierre diario por Concentrador % - Desde ayer	100%	19/12/2016 12:01:48
Cierre diario por Concentrador % - Última semana	100%	19/12/2016 12:02:24
Perfil de carga por Concentrador % - Ayer	100%	19/12/2016 12:01:01
Perfil de carga por Concentrador % - Última semana	86%	19/12/2016 12:04:32
Tamaño de ficheros por Concentrador (kB) - Ayer	47,43359	19/12/2016 12:00:45
Tamaño de ficheros por Concentrador (kB) - Mes en curso	300,3359	19/12/2016 09:00:53

Elementos mostrados 1 - 13 de 13

Figura 102 – Estadísticas del concentrador

Para visualizar una estadística en detalle hay que hacer clic sobre ella. De este modo se mostrará un histórico de la misma.

2.2.10 Histórico de Ping

Esta pestaña muestra las estadísticas relativas a los intentos de ping al concentrador en cuestión. Se muestran todos los pings, indicando en cada uno su fecha y su resultado (fallido o exitoso). Como en otras pestañas, también podemos filtrar por intervalos de tiempo.

Las estadísticas se muestran también en forma de gráfica en la parte superior.

☆ **Número de Serie del Concentrador: ZIV0004372798**

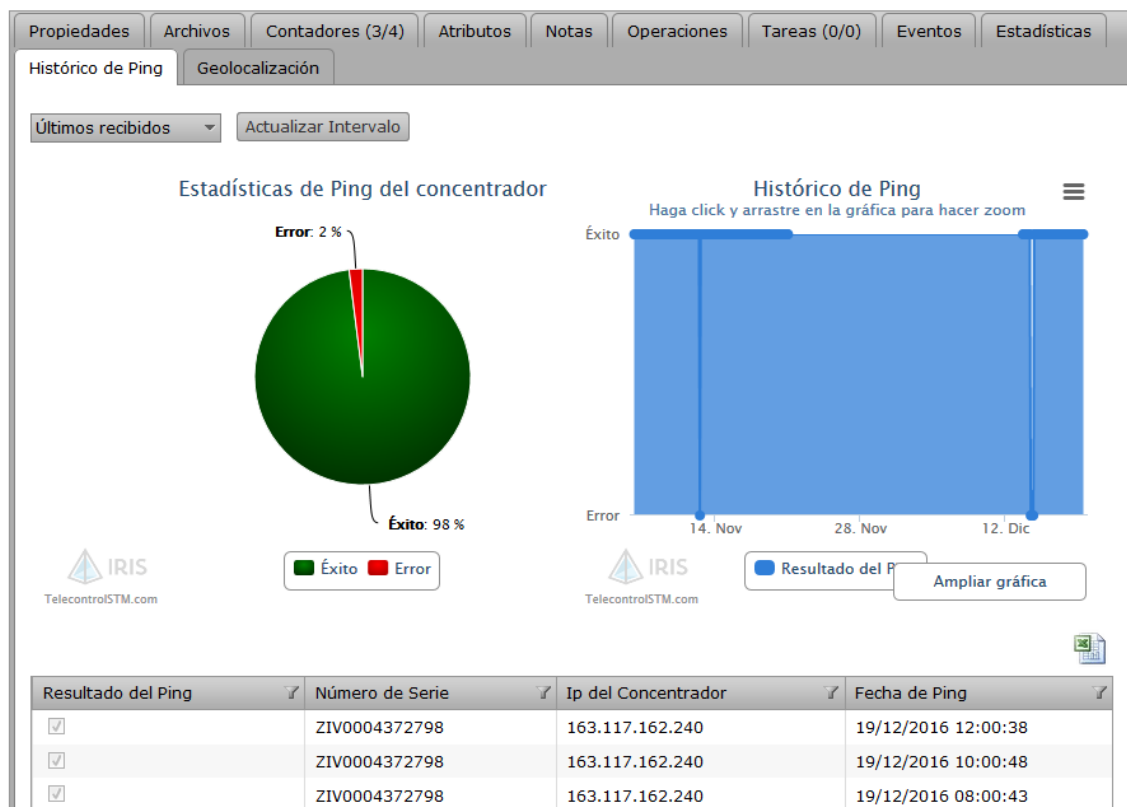


Figura 103 – Histórico de ping del concentrador

2.2.11 Geolocalización

Esta pestaña muestra la ubicación del concentrador (representado como una estrella dorada) con sus concentradores en el mapa y nos da la posibilidad tanto de modificar la ubicación de un concentrador ya existente como de ubicar un nuevo concentrador. La ubicación del concentrador aparece marcada con una estrella dorada, con todos sus contadores marcados como que, dependiendo del color, pueden estar activos (color verde), en fallo temporal (color amarillo), en fallo permanente (color rojo) o sin información (color gris).

☆ Número de Serie del Concentrador: **VDC-000001**

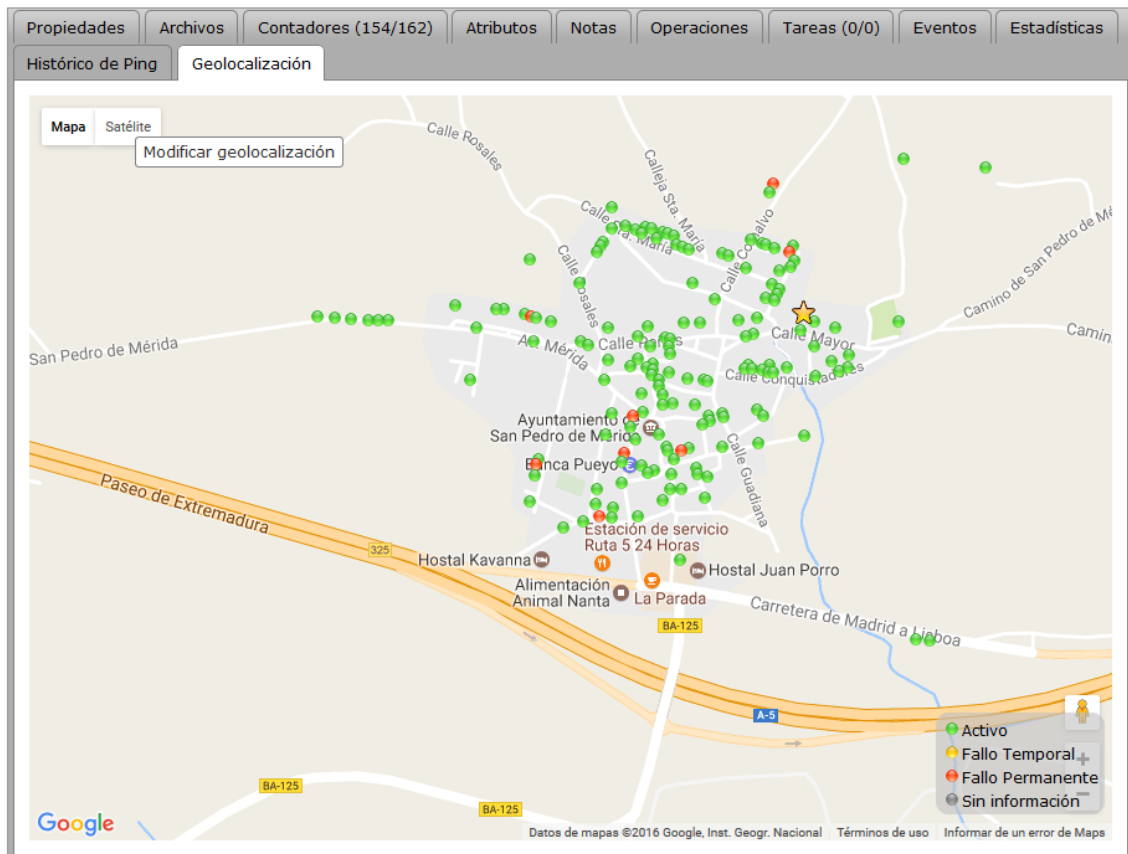


Figura 104 – Geolocalización del concentrador y sus contadores asociados

Para cambiar la geolocalización de un concentrador hay que hacer clic en “Modificar geolocalización”, introducir sus coordenadas (latitud y longitud), bien por teclado o bien haciendo clic en el mapa en el punto deseado y hacer clic por último en “Guardar”.

2.2.12 Contadores

Hemos dejado la pestaña “Contadores” por ser la más extensa e importante, ya que es a través de la cual podemos acceder a todos los contadores asociados al concentrador seleccionado y desde donde podremos llevar a cabo la gestión de estos.

☆ Número de Serie del Concentrador: **ZIV0004372798**

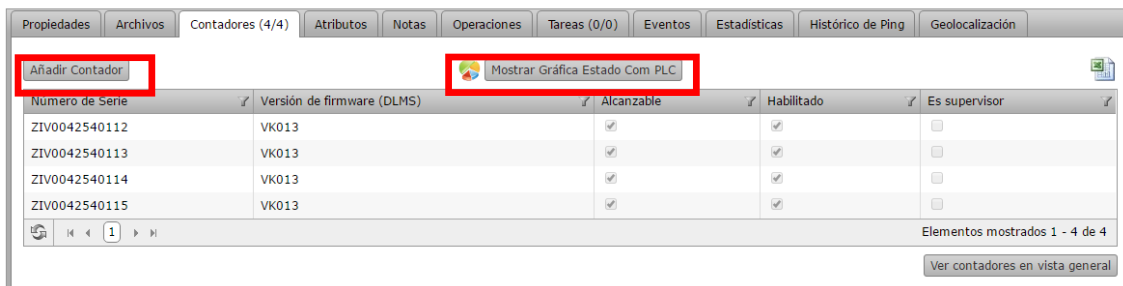


Figura 105 – Contadores asociados a un concentrador

Aquí tenemos la posibilidad de añadir nuevos contadores y de ver el estado de la comunicación de los contadores asociados al concentrador seleccionado. Seleccionando un grupo de contadores se muestran las operaciones disponibles sobre ellos, que son exactamente las mismas que sobre los concentradores. Haciendo clic en uno de los contadores se nos muestran en pantalla los atributos de dicho contador. Como podemos ver, esta pantalla es muy similar a la anteriormente mostrada para los concentradores.

2.2.12.1 Propiedades



Figura 106 – Propiedades del contador

El interruptor verde de la esquina superior izquierda (2) nos indica que el contador está conectado. Haciendo clic sobre “Cambiar” (3) es posible cambiar el concentrador asociado a este contador introduciendo su número de serie.

Las propiedades del contador que no sean meramente informativas pueden ser modificadas. La propiedad “Es supervisor” no es modificable. Cuando un contador es

supervisor suele colocarse junto al concentrador o incluso dentro de él, ya que la mayoría de los concentradores tienen la funcionalidad de contador interno, y su objetivo es el detectar posibles fraudes ya que este contador toma medidas de la red completa, por lo que si la medida de este contador no coincide con la suma de las medidas de todos los contadores de la red (teniendo en cuenta que nunca será idéntica debido a las pérdidas), podría plantearse un caso de posible fraude. En la parte inferior se muestran las opciones de eliminar el contador, ver a qué colecciones pertenece y añadir dicho contador a una colección. En la parte superior aparece el número de serie del contador y el de su concentrador asociado (4), en el caso de que lo tenga, ya que de otro modo estaríamos hablando de un contador huérfano.

El indicador situado en la parte superior junto al número de serie del contador indica la cobertura PLC del mismo (1). Este indicador solamente mostrará el nivel de cobertura cuando se hayan recibido estadísticas PLC del contador en cuestión en las últimas 12 horas.



Diferentes estados del indicador de cobertura PLC.

En la parte de la derecha aparece la información acerca de las tarifas contratadas por el contador y la potencia correspondiente a cada una (5).

2.2.12.2 Perfiles de carga (S02)

Seleccionando la opción “Perfiles de carga (S02)” se muestran los valores horarios de consumo del contador.

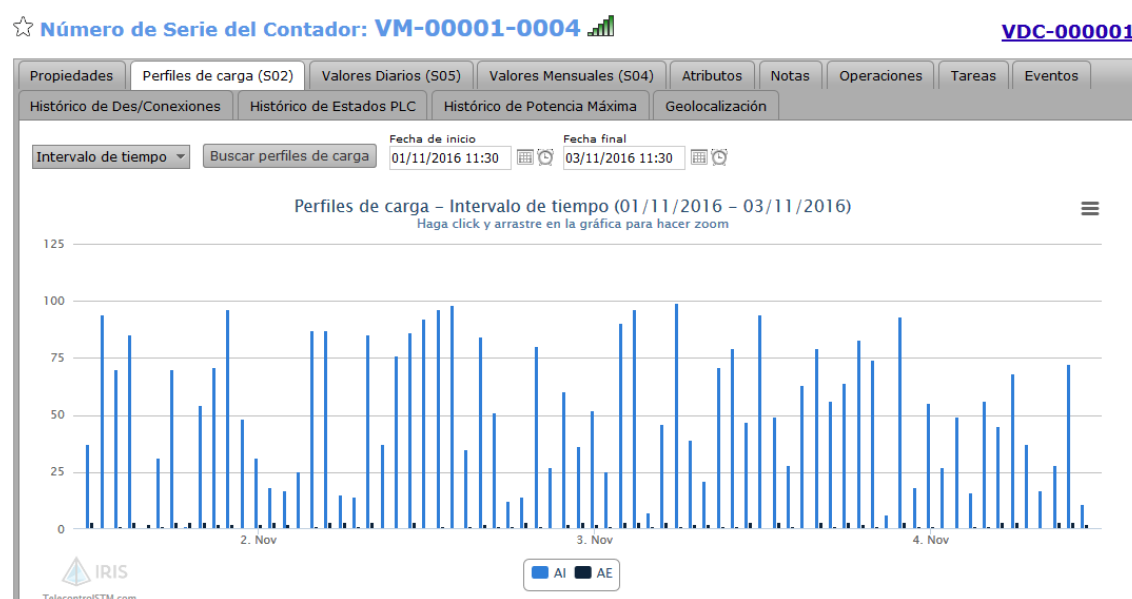


Figura 107 – Perfiles de carga horarios por intervalo de tiempo del contador

Dichos perfiles de carga pueden ser buscados para un intervalo de tiempo, como en la imagen, en la que se realiza una búsqueda entre el día 24 y el 27 de marzo. También se pueden buscar los perfiles de carga para el último día, semana, mes o últimos recibidos.

Debajo de esta gráfica se muestra una tabla en la que se ven los mismos datos de consumo.

Fecha	Consumo reactivo (AE)	Consumo (AI)	Bit de calidad (Bc)
01/11/2016 12:00:00	3 W/h	37 W/h	1
01/11/2016 13:00:00	0 W/h	94 W/h	1
01/11/2016 14:00:00	1 W/h	70 W/h	1
01/11/2016 15:00:00	3 W/h	85 W/h	1
01/11/2016 16:00:00	2 W/h	0 W/h	1
01/11/2016 17:00:00	1 W/h	31 W/h	1
01/11/2016 18:00:00	3 W/h	70 W/h	1
01/11/2016 19:00:00	3 W/h	1 W/h	1
01/11/2016 20:00:00	3 W/h	54 W/h	1
01/11/2016 21:00:00	2 W/h	71 W/h	1
01/11/2016 22:00:00	2 W/h	96 W/h	1
01/11/2016 23:00:00	0 W/h	48 W/h	1
02/11/2016 00:00:00	2 W/h	31 W/h	1
02/11/2016 01:00:00	3 W/h	18 W/h	1
02/11/2016 02:00:00	2 W/h	17 W/h	1
02/11/2016 03:00:00	0 W/h	25 W/h	1
02/11/2016 04:00:00	1 W/h	87 W/h	1
02/11/2016 05:00:00	2 W/h	87 W/h	1

Figura 108 – Perfiles de carga horarios por intervalo de tiempo del contador

2.2.12.3 Valores diarios (S05)

Este apartado muestra los valores diarios de consumo del contador.

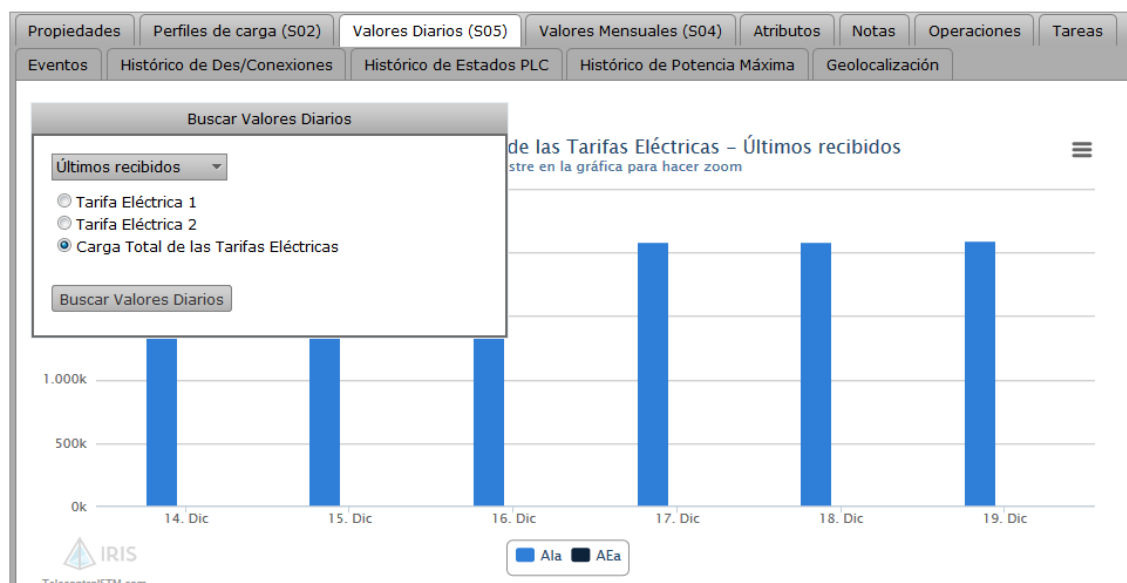


Figura 109 – Valores diarios de consumo del contador

En este apartado también es posible seleccionar el intervalo de tiempo en el que queremos que se nos muestren los valores diarios. También se puede mostrar el consumo filtrándolo por tarifa, ya sea “*Tarifa Eléctrica 1*” o “*Tarifa Eléctrica 2*”, con el fin de ver el consumo detallado de cada una de ellas.

Al igual que en el caso de los perfiles de carga, también se puede ver el consumo diario en forma de tabla, y esta se encuentra inmediatamente debajo de la gráfica.

2.2.12.4 Valores mensuales (S04)

En la línea de los dos apartados anteriores, aquí también se muestran los valores del contador por franja de tiempo, en este caso por mes.

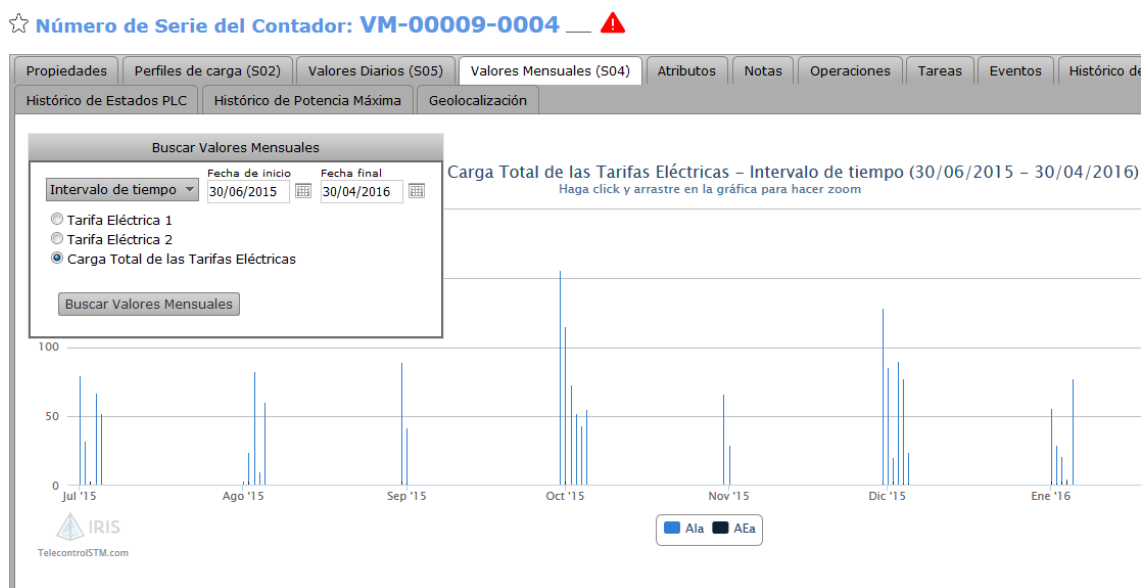


Figura 110 – Valores de consumo mensuales del contador

Como se puede apreciar, los mecanismos de búsqueda son similares a los anteriormente mostrados.

Como en los casos anteriores, debajo de esta gráfica se muestra una tabla con la información sobre el consumo.

2.2.12.5 Atributos y Notas

Estas dos pestañas funcionan de manera idéntica a las pestañas “Atributos” y “Notas” de los concentradores, que han sido analizadas anteriormente.

2.2.12.6 Operaciones

Como ya se ha visto anteriormente con los concentradores, los contadores tienen también su propia pestaña para lanzar operaciones sobre ellos.



Figura 111 – Operaciones del contador

Como se puede ver, las distintas operaciones se dividen a su vez en “Peticiones”, “Eventos”, “Órdenes” e “Informes”.

Mediante la opción “Peticiones” es posible solicitar al contador estadísticas e información acerca de su funcionamiento, como por ejemplo sus parámetros, valores instantáneos o curva de carga diaria.

La opción “Eventos” permite consultar los eventos de diferente tipo que han tenido lugar en el contador, como es el caso de los eventos de fraude.

El apartado “Órdenes” es el que va a permitir realizar los principales cambios en la configuración de los contadores, ya que nos permiten, por ejemplo, cambiar la tarifa de los contadores, conectarlos y desconectarlos. Dos de las órdenes más importantes son “Configurar la potencia máxima (B02)”, mediante la cual podremos escoger entre los valores de potencia establecidos, y “Reconectar/Desconectar”, mediante la cual se corta/restablece el suministro del contador en cuestión.

Seleccionando el informe “Curva de carga”, IRIS genera un fichero pdf con información del contador.

2.2.12.7 Tareas y eventos

Estas dos pestañas funcionan exactamente igual que en el caso de los concentradores.

2.2.12.8 **Histórico de Estados PLC**

Esta pestaña muestra los diferentes estados PLC por los que ha pasado el contador seleccionado. Se pueden aplicar filtros por intervalos de tiempo y buscar cambios de registro concretos. La información relativa a los estados PLS aparece en forma de tabla en la parte inferior y también en forma de gráficas en la parte superior.

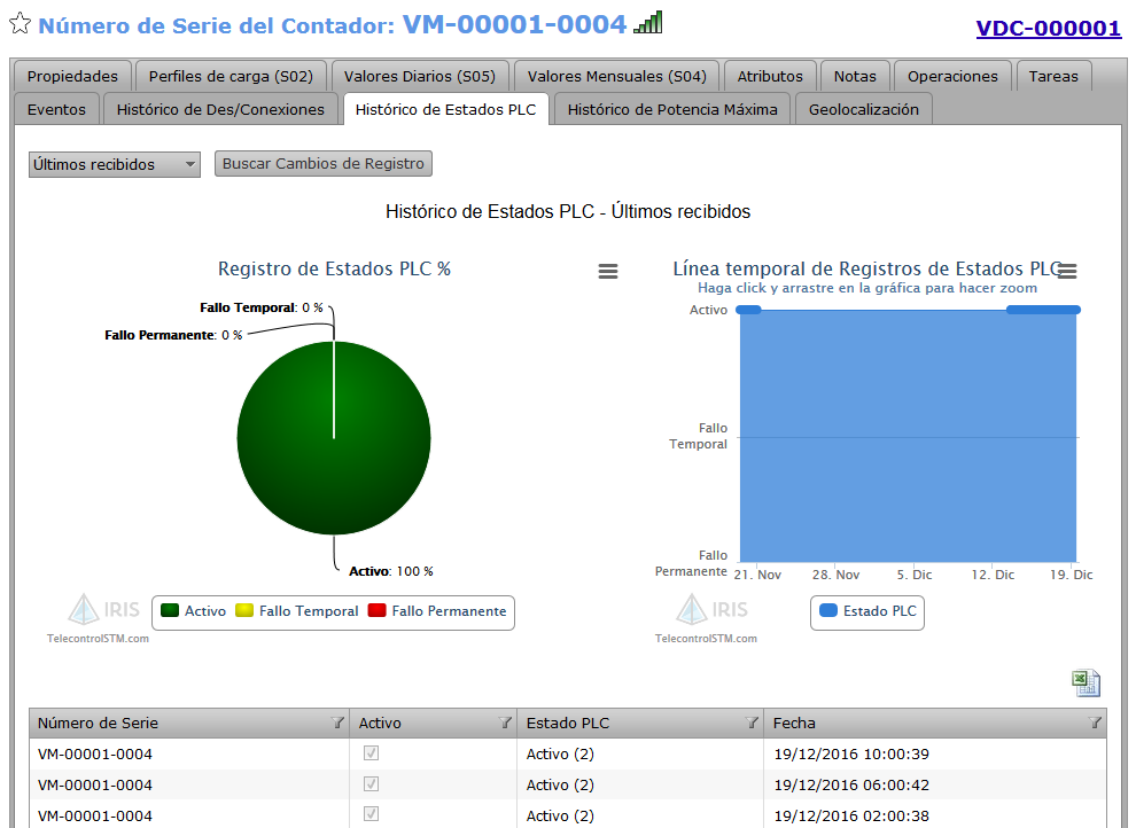


Figura 112 – Histórico de estados PLC del contador

2.2.12.9 **Histórico de Potencia Máxima**

Aquí podemos ver los valores de potencia máxima que ha tenido el contador a lo largo del tiempo dependiendo del tipo de tarifa contratada.

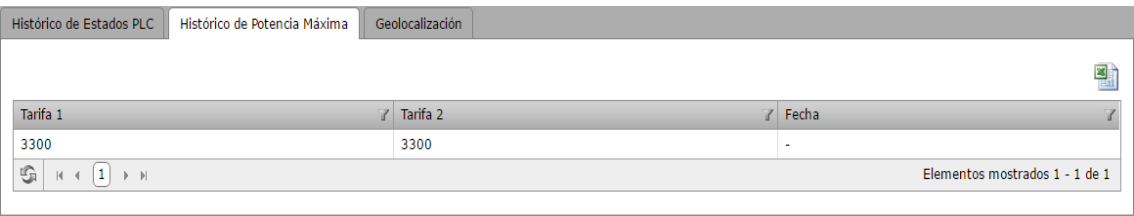


Figura 113 – Histórico de potencia máxima del contador

2.2.12.10 Geolocalización

En esta pestaña será posible ver la ubicación exacta del contador en Google Maps. Podremos ubicar los nuevos contadores, así como modificar la localización de los contadores ya instalados.

2.2.12.11 Contadores huérfanos

Un contador se considera como *huérfano* cuando no está asociado a ningún concentrador o está registrado en un concentrador que no conoce. Un contador se puede encontrar en esta situación cuando:

- Se ha eliminado su concentrador.
- Se ha agregado un contador y aún no sabe su concentrador.

3. Colecciones

Las colecciones nos permiten agrupar múltiples dispositivos (ya sean concentradores o contadores) bajo un mismo nombre. Las colecciones se dividen en colecciones de usuario y colecciones de sistema.

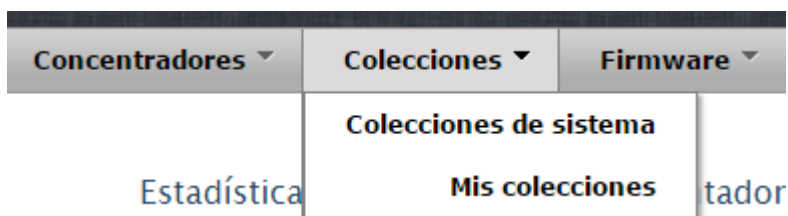


Figura 114 – Colecciones en IRIS

3.1 Colecciones de usuario

Estas colecciones son las que han sido creadas por un usuario para su uso particular. Estas colecciones solo podrán ser vistas por el propio usuario que las ha creado. Para acceder a ellas solamente hay que hacer clic en “*Mis colecciones*”.

Para añadir una nueva colección basta con seleccionar “*Añadir Colección*”, indicar el nombre que le queremos dar y, por último, hacer clic en “*Añadir Colección*”.

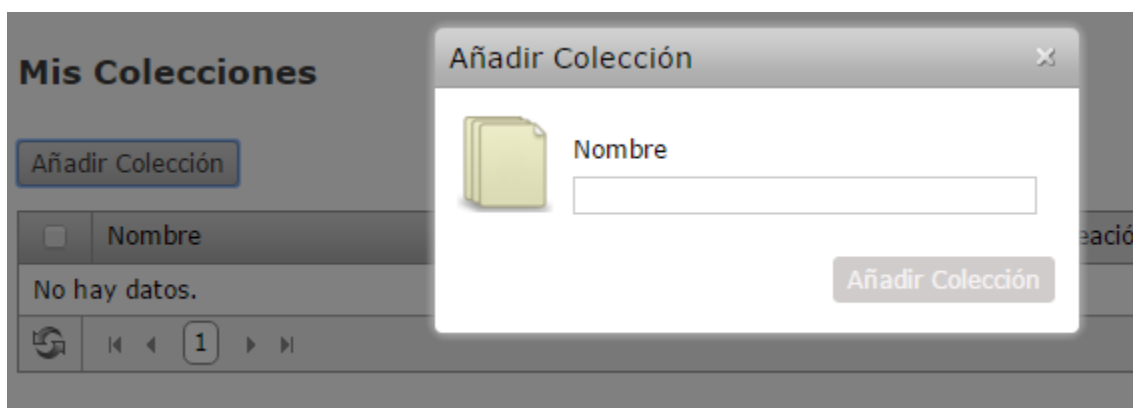


Figura 115 – Añadir colección de usuario

Para eliminar una o varias colecciones hay que marcar dichas colecciones y hacer clic en la opción “*Eliminar Colección*”, que aparecerá en ese momento en la parte inferior. Aparecerá un mensaje de confirmación y, después de hacer clic en “*Borrar colección/es*”, la eliminación se hará efectiva.

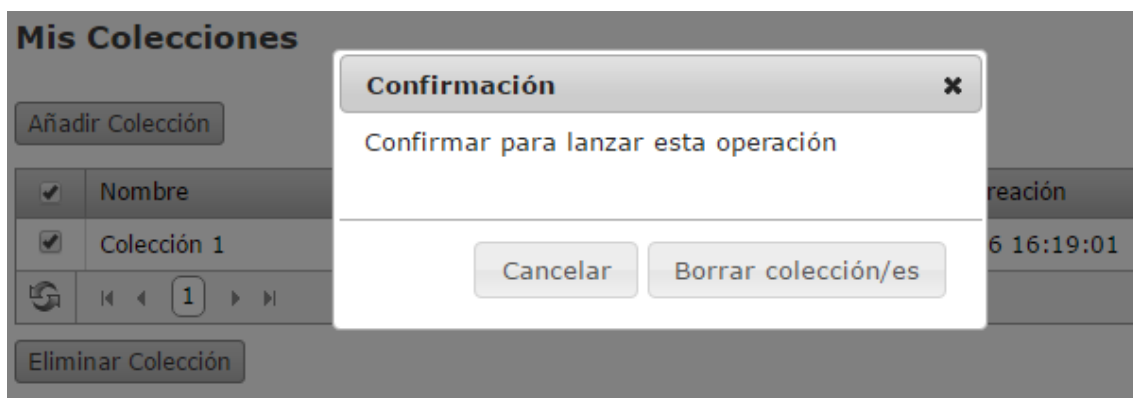


Figura 116 – Borrar colección de usuario

Al seleccionar una colección de usuario se abrirán tres nuevas pestañas: “Propiedades”, “Concentradores” y “Contadores”.

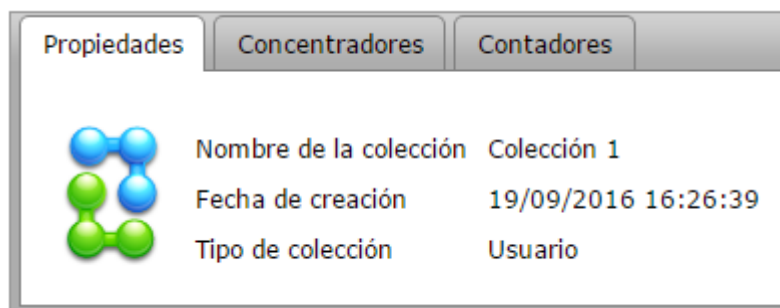


Figura 117 – Información de colección de usuario

La pestaña “Propiedades” nos muestra un resumen de las características de la colección. Los dispositivos pertenecientes a esta colección se pueden ver en las pestañas “Concentradores” y “Contadores”.

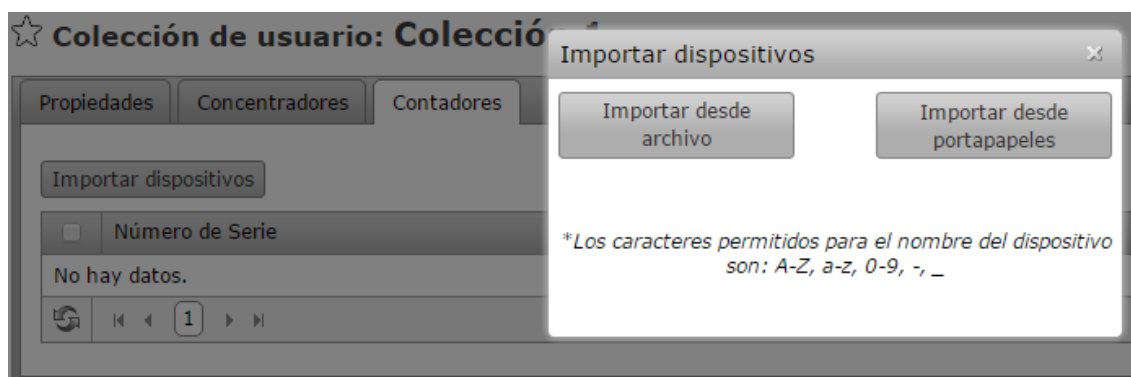


Figura 118 – Añadir dispositivos a una colección de usuario

Desde las pestañas “Concentradores” y “Contadores” podemos añadir nuevos dispositivos a la colección seleccionando “Importar dispositivos”. Al mismo tiempo, tenemos dos formas de importar estos dispositivos.

La primera opción es “Importar archivos”, mediante la cual podremos importar archivos .txt o .csv. Sólo se tomarán como válidos aquellos nombres que estén compuestos por los caracteres A-Z, a-z, 0-9, -, _.

La segunda opción es “Importar desde portapapeles”. Con esta opción podremos introducir manualmente el número de serie o conjunto de números de serie.

Hay que tener en cuenta que estos mecanismos solo funcionarán si los números de serie introducidos ya existen en el sistema IRIS.

3.2 Colecciones de sistema

Estas colecciones tienen carácter general, todos los usuarios del sistema podrán acceder a ellas. Además, en estas colecciones disponemos de una pestaña adicional con respecto a las colecciones de usuario: la pestaña de “Estadísticas”. Esta pestaña nos mostrará información relativa a los dispositivos que componen la colección.

4. Firmware

En esta opción tendremos todas las versiones de firmware disponibles en el sistema. Para descargar un firmware concreto bastará con hacer clic sobre él.



Figura 119 – Pestaña “Firmware”

También tenemos la opción de añadir nuevo firmware haciendo clic sobre la opción “Añadir nuevo firmware” y también la de eliminar los ya existentes.



Figura 120 – Gestión de firmwares

5. Sistema

Este menú está compuesto por cuatro secciones diferentes: “Operaciones”, “Tareas”, “Estadísticas” y “Potencias”.

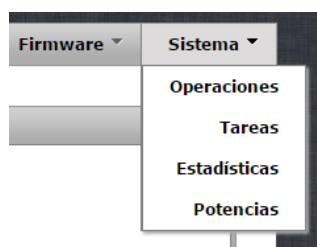


Figura 121 – Pestaña “Sistema”

5.1 Operaciones

Al pulsar en “Operaciones” aparecen los distintos tipos que están disponibles en IRIS: “Informes”, “Estadísticas”, “Tareas” y “Dispositivos”.



Figura 122 – Operaciones del sistema

5.2 Tareas

En la pestaña “Tareas” se muestra una tabla con las tareas del sistema, así como su estado (en curso, finalizada, etc.) y demás información relativa a ellas, al estilo de la pestaña que muestra las tareas de los concentradores, que se ha visto antes.

5.3 Estadísticas

En esta pestaña se muestra un conjunto de estadísticas relativas al sistema IRIS completo. Haciendo clic sobre cada una de estas estadísticas podemos ver el histórico de la misma, al igual que en las estadísticas de los contadores.

Operaciones	Tareas	Estadísticas	Valores de Potencia Actuales
Últimas estadísticas del sistema			
Recalcular estadísticas			
Nombre de la Estadística	Valor de la Estadística	Fecha	
Número de contadores	1593	19/12/2016 12:00:18	
Número de concentradores	11	19/12/2016 12:00:18	
Concentradores con éxito en el último ping %	91%	19/12/2016 12:00:12	
Nº de archivos - Ayer	941	19/12/2016 12:00:31	
Nº de archivos - Hoy	433	19/12/2016 12:00:31	
Concentradores que enviaron un S24 - Ayer	10	19/12/2016 12:00:38	
Cierre diario % - Hoy	100%	19/12/2016 12:01:41	
Cierre diario % - Ayer	100%	19/12/2016 12:02:20	
Cierre diario % - Últimos 7 días	100%	19/12/2016 12:02:43	
Concentradores con éxito en el último ping	10	19/12/2016 12:00:12	
Concentradores con fallo en el último ping	1	19/12/2016 12:00:12	
Contadores inactivos en la red PLC del último día	65	19/12/2016 12:00:38	
Contadores con fallo temporal en la red PLC del último día	0	19/12/2016 12:00:38	
Contadores activos en la red PLC del último día	1363	19/12/2016 12:00:38	
Perfil de carga % - Ayer	100%	19/12/2016 12:04:23	
Perfil de carga % - Últimos 7 días	86%	19/12/2016 12:04:45	
Número de contadores huérfanos	165	19/12/2016 12:00:41	
Elementos mostrados 1 - 17 de 17			

Figura 123 – Estadísticas del sistema

5.4 Valores de potencia actuales

Esta pestaña muestra todos los valores de potencia disponibles para ser aplicados sobre los contadores. Desde aquí podemos también introducir nuevos valores de potencia.

Valores de Potencia Actuales	
660 ✖	5500 ✖
770 ✖	6600 ✖
1100 ✖	7700 ✖
1650 ✖	8800 ✖
2200 ✖	9900 ✖
3300 ✖	11000 ✖
4400 ✖	13860 ✖

Figura 124 – Valores de potencia actuales en el sistema

ANEXO IV

Manual de usuario de ZIV PRIME Manager

El sniffer ZIV PRIME Manager es la herramienta que nos va a permitir capturar tráfico intercambiado entre el concentrador y sus contadores asociados.

Para conectarnos al sniffer y comenzar a capturar tráfico, solamente habrá que hacer que seleccionen la opción “Connect To...” mediante cualquiera de las opciones, (1) y (2), que se muestran en la figura de debajo, ya que ambas son equivalentes.

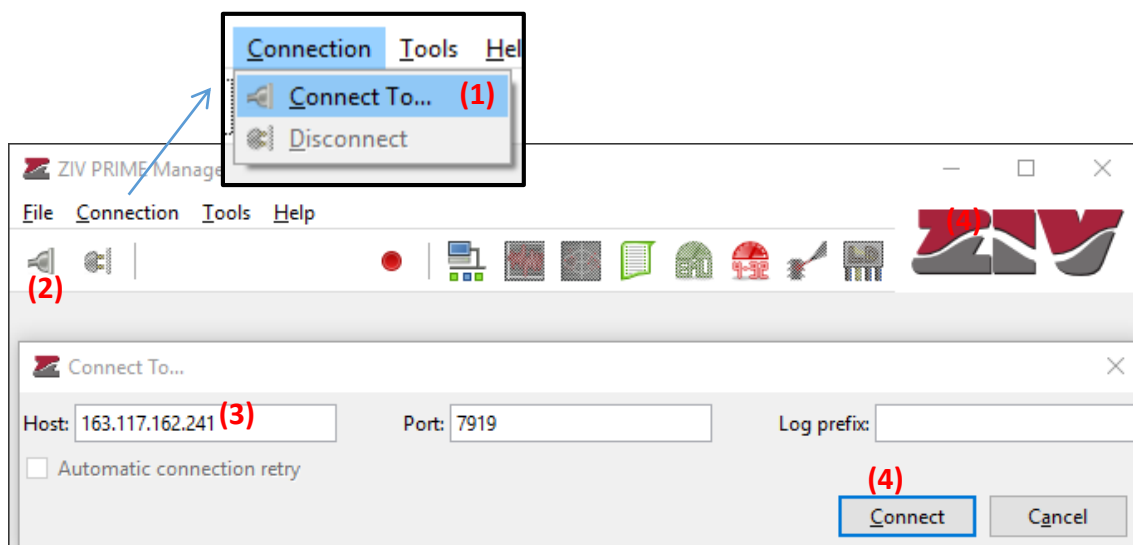


Figura 125 – Conexión de ZIV PRIME Manager

Una vez hayamos seleccionado esta opción hay que introducir la dirección IP a la que nos queremos conectar (3) y conectarse (4).

Una vez estemos conectados, ya podemos empezar a capturar tráfico, pero antes hay que seleccionar el tipo de información que queremos que se nos muestre por pantalla. La primera opción que tenemos es la de mostrar la información del dispositivo (sniffer ZPM). Para ello seleccionamos la opción “Device information” (1).

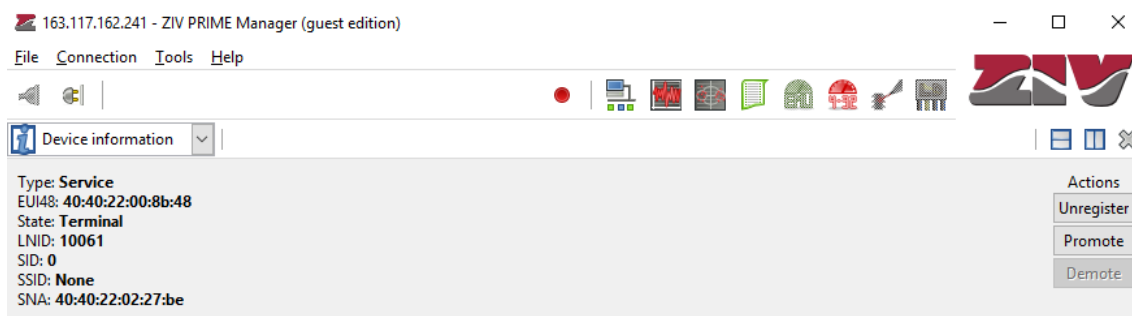


Figura 126 – Información del sniffer ZPM

Aquí se mostrarán las direcciones MAC (EUI48) y su SNA (SubNetwork Address) que coincide con la MAC del concentrador. Podemos ver claramente que el sniffer se está comportando como un service node más en estado terminal y con LNID asignado. Por tanto, a efectos de intercambio de tráfico con el concentrador sería un contador más. Al tratarse de un nodo más de la subred, tenemos la opción de cancelar su registro (2), promocionarlo para que pase a estado switch (3) y degradarlo después para que vuelva al estado terminal (4).

Para capturar capturar tramas MAC, seleccionamos la opción de visualización “MAC PDUs” (1) y, posteriormente, indicar el tipo de tráfico que queremos capturar mediante la opción “Capture MAC PDUs” (2).



Figura 127 – Captura de MAC PDUs

A partir de este momento, comenzaremos a capturar tráfico. Para detener la captura, únicamente habrá que pulsar otra vez sobre “Capture MAC PDUs” (6).

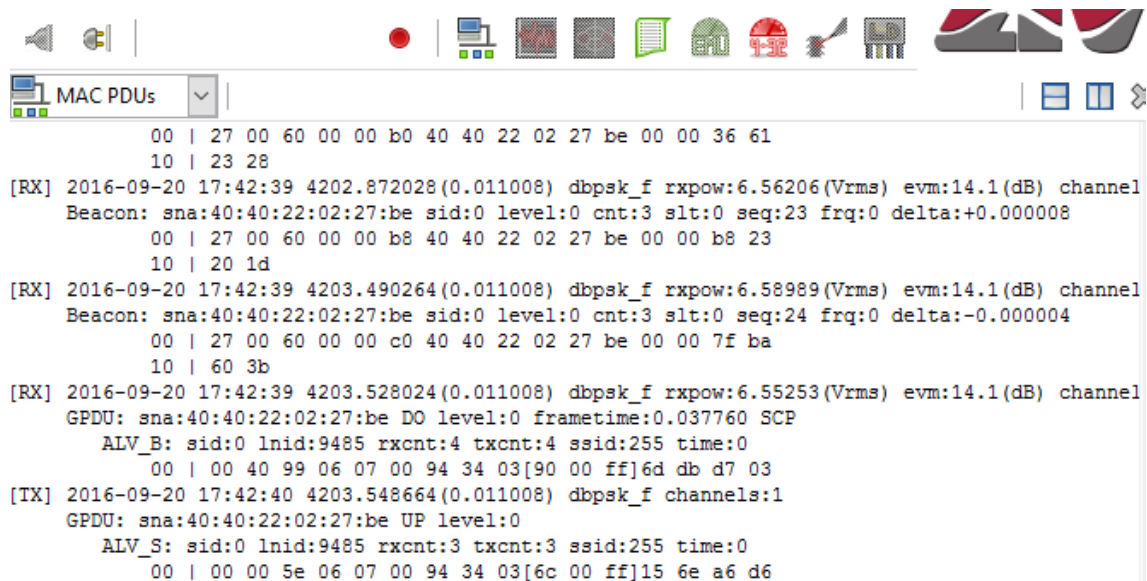


Figura 128 – Tráfico capturado

Tenemos también la opción de ver la constelación que de la modulación utilizada por PRIME. Para ello hay que seleccionar “Capture PHY IQ” (1) y en las opciones de visualización seleccionamos “PHY IQ” (2).

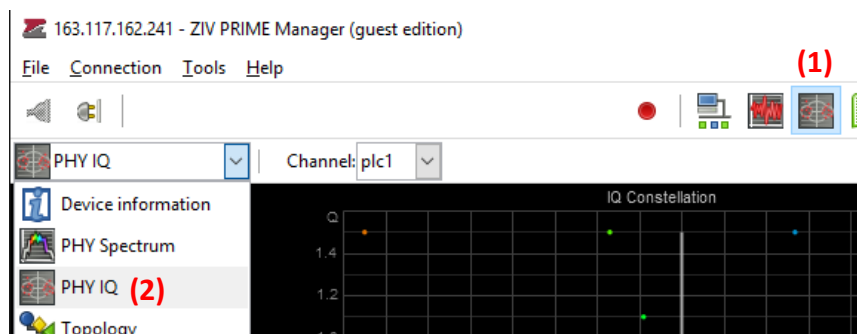


Figura 129 – Pasos para mostrar la constelación

Una vez accedamos a la visualización de la constelación deberemos seleccionar el canal (plc1) y se mostrará claramente la constelación utilizada por PRIME.

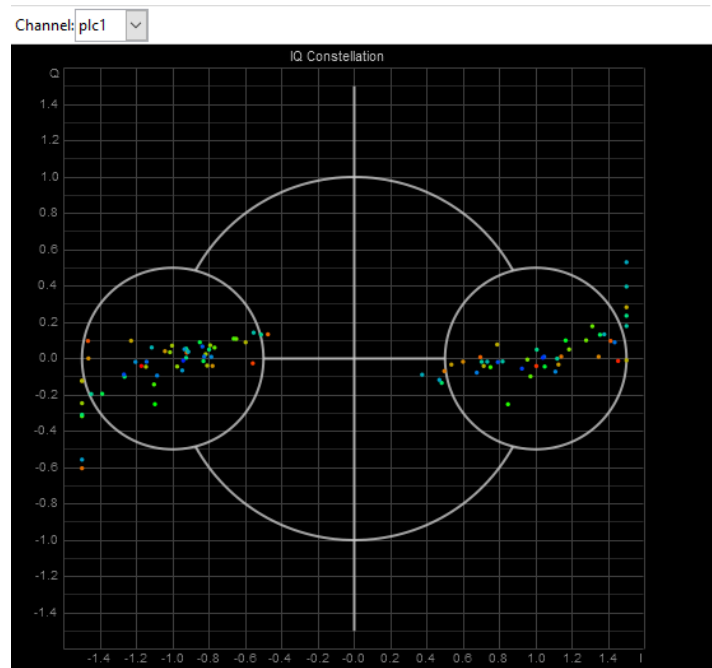


Figura 130 – Constelación de la modulación utilizada por PRIME

Otra de las opciones que tenemos con ZIV PRIME Manager es la de mostrar el rango de frecuencias en el que trabaja PRIME. Para ello tenemos que seleccionar “Capture PHY samples” (1) y “PHY Spectrum” (2) en el modo de visualización.

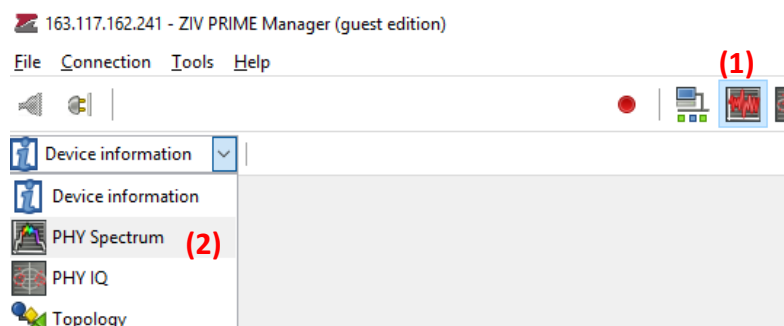


Figura 131 – Pasos para mostrar el rango de frecuencias

El rango de frecuencias en el que trabaja PRIME aparece coloreado.

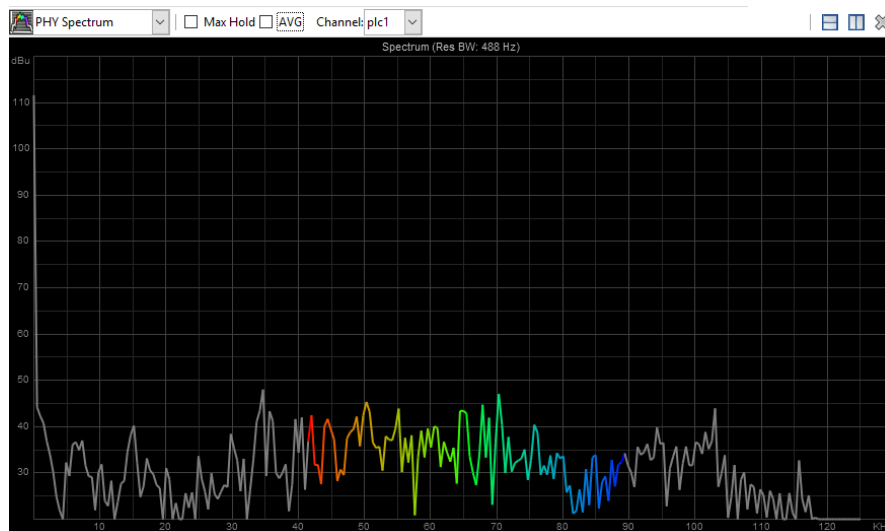


Figura 132 – Rango de frecuencias de PRIME

Para tener una visión más clara de cómo se comporta PRIME en frecuencia podemos seleccionar las casillas de la parte superior “Max. Hold”, para que los picos de actividad queden marcados en la gráfica, y “AVG”, para que los valores de intensidad se muestren en media y las oscilaciones sean menos bruscas.

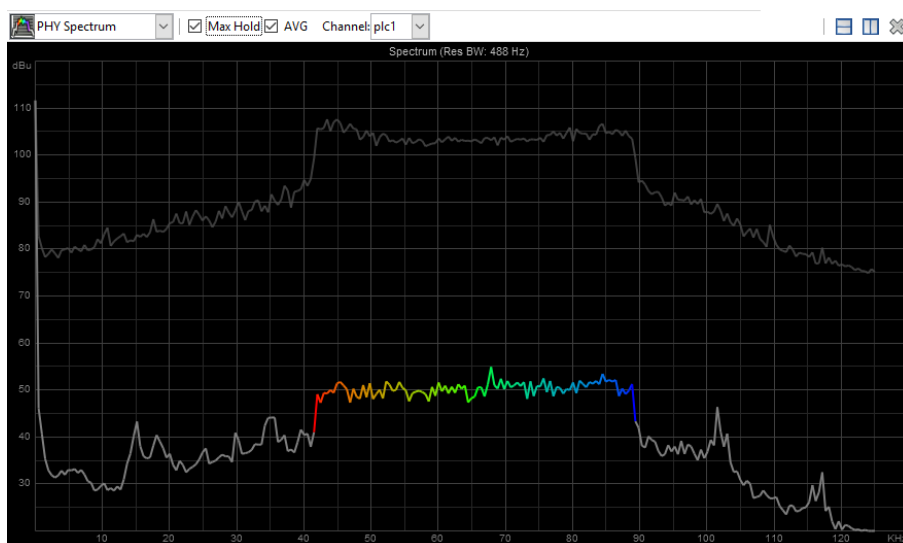


Figura 133 – Rango de frecuencias de PRIME en media y con máximo mantenido

ANEXO V

Manual de usuario de la Interfaz Web del Concentrador ZIV

La interfaz web del concentrador ZIV nos va a permitir nos va a permitir configurar el concentrador y establecer comunicación entre éste y los contadores en tiempo real. Desde aquí podemos solicitar diferentes informes y estadísticas al propio concentrador o a cualquiera de sus contadores asociados.

Para acceder a esta interfaz web, solamente hay que introducir la dirección ip del concentrador ZIV en la barra de búsqueda del navegador e introducir el nombre de usuario y contraseña.

Una vez que estemos dentro de la interfaz, seleccionando “*Operation*” podemos solicitar los informes relativos al concentrador y su funcionamiento. Estos informes son los que vemos en la siguiente imagen y entre ellos se encuentran solicitar la lista de contadores asociados al concentrador (S20), parámetros del contador (S12), información PLC (S11), etc.



Figura 134 – Informes del concentrador ZIV

Dentro del menú “Operation” tenemos la opción de ver la lista de contadores asociados al concentrador en cuestión, así como el estado en el que se encuentran, seleccionando “Meter list”.

Meter list									
Return Reload Clear all Clear PF Synchronize Cancel all Restore keys									
#	Serial	MAC	Version	Prime version	Present	Last communication	Status changes	Active time	Tracking
1	ZIV0042540112	40:40:22:89:1c:50	VK013	V2203	TF	2016/09/26 16:35:18	0	100.00%	Add
2	ZIV0042540113	40:40:22:89:1c:51	VK013	V2203	A	2016/09/26 04:00:06	0	100.00%	Add
3	ZIV0042540114	40:40:22:89:1c:52	VK013	V2203	A	2016/09/26 04:00:12	2	100.00%	Add
4	ZIV0042540115	40:40:22:89:1c:53	VK013	V2203	A	2016/09/26 04:00:16	2	100.00%	Add

Figura 135 – Lista de contadores del concentrador ZIV

Como se puede ver, hay tres contadores encendidos y uno apagado (el primero de la lista). Seleccionando cualquiera de los contadores encendidos se nos mostrarán los diferentes informes y operaciones que podemos solicitar sobre ese contador en concreto. En los contadores apagados también podemos realizar ciertas acciones, pero muchas de ellas no están disponibles.

Operation

- [Meter list](#)
 - ZIV0042540113
- [Report stats](#)
- [Order stats](#)
- [XML cycles](#)
- [DLMS reflash](#)

PRIME

Configuration

Statistics

- [Apply](#)
- [Save](#)
- [Reboot](#)
- [Reflash](#)
- [Configuration files](#)

Meter overview: ZIV0042540113


[Return to list](#)

Serial number	ZIV0042540113
MAC	40:40:22:89:1C:51
Version	VK013
Prime version	V2203
Present	A
ARQ	yes
Status changes	0
Active time	100.00%
Profiles DB (S02)	Stored 744 items from 2016/08/26 05:00:00 to 2016/09/26 04:00:00 TpCompl not initialized
Monthly billing DB (S04)	Stored 9 items from 2016/01/01 00:00:00 to 2016/09/01 00:00:00 TpCompl not initialized
Daily billing DB (S05)	Stored 93 items from 2016/06/15 00:00:00 to 2016/09/26 00:00:00 TpCompl not initialized

- [Details](#)
- [Control](#)
- [Profiles graph](#)
- [Instant values \(S01\)](#)
- [Profiles \(S02\)](#)
- [Daily absolutes \(S03\)](#)
- [Monthly billing \(S04\)](#)
- [Daily billing \(S05\)](#)
- [Meter parameters \(S06\)](#)
- [Power failure \(S07\)](#)
- [Power quality \(S08\)](#)
- [Events \(S09\)](#)
- [Voltage and cur. prof. \(S14\)](#)
- [Advanced instant values \(S21\)](#)
- [Activity calendar \(S23\)](#)
- [Instant vals. on dem. \(S26\)](#)
- [Current billing \(S27\)](#)

Figura 136 – Informes de contador


En el menú que se abre al seleccionar un contador podemos ver cierta información relativa al contador, así como los diferentes informes que podemos solicitarle. Para solicitar un informe solamente habrá que hacer clic sobre dicho informe.

 **Profiles (S02): ZIV0042540113**

Start date	<input type="text" value="2016/09/25 16:45:54"/>
End date	<input type="text" value="2016/09/26 16:45:54"/>
Source	<input type="text" value="Meter"/>

Figura 137 – Opciones del informe de contador

Es importante marcar el campo “Meter” en la opción “Source” y, posteriormente, seleccionamos “Request” para solicitar el informe. En ese momento comienza el proceso en el que el concentrador y el contador intercambian la información necesaria para generar el informe y que, por lo general, no debe ser superior a unos segundos. Cuando el informe se ha generado correctamente aparecerá un mensaje que indica que el proceso ha finalizado, y un enlace con el nombre del informe en el que haciendo clic tenemos la posibilidad de guardar el informe en formato XML.

 **Profiles (S02): ZIV0042540113**

● Report finished

[S02.xml](#)

Figura 138 – Informe de contador finalizado

Para solicitar cualquier tipo de informe el procedimiento es idéntico al mostrado.

Volviendo a la página de inicio de la interfaz web del concentrador ZIV, se vuelven a ver las opciones que aparecen a la izquierda. En este caso seleccionamos la opción “PRIME”.

Operation

PRIME

Database file

Topology evolution

Configuration

Statistics

Apply

Save

Reboot

Reflash

Configuration files

PRIME interfaces

MAC	Address	Channel	Registered
40:40:22:02:27:be	phy	5	
Total		5	

PRIME topology

Serial	MAC	SID	LNID	State	SSID	Coverage	Conn. time	Disc. time	Availability	
<div><div></div><div></div><div></div><div></div><div></div></div>		40:40:22:02:27:be	-	-	Base	0				
		00:80:e1:32:48:5c	0	8502	Disconnected	-		09-10 14:23	09-10 14:25	00%
	ZIV0042540114	40:40:22:89:1c:52	0	8983	Terminal	-	<div></div>	09-10 18:48	09-10 19:15	87%
	ZIV0042540113	40:40:22:89:1c:51	0	9420	Terminal	-	<div></div>	09-10 10:05	09-10 19:15	87%
	ZIV0042540115	40:40:22:89:1c:53	0	9451	Terminal	-	<div></div>	09-09 03:48	09-10 19:15	87%
		40:40:22:00:8b:48	0	9705	Terminal	-	<div></div>	09-10 18:48	09-10 19:15	60%
ZIV0042540112	40:40:22:89:1c:50	0	10176	Terminal	-	<div></div>	09-10 19:14	09-10 19:15	93%	

Reload

Download as .csv


Figura 139 – Dispositivos de la subred

Aquí podemos ver todos los equipos (ya que no son sólo contadores y, como se puede ver aparece una dirección MAC sin número de serie asociado que pertenece al sniffer) asociados al concentrador, así como su información básica como su LNID, cobertura PLC, si el nodo es terminal o switch, etc. Seleccionando cualquiera de ellos se muestra esta misma información de manera individual, como se puede ver en la siguiente figura.


PRIME node details	
<input type="button" value="Return to PRIME tree"/>	
Serial Number	ZIV0042540113
MAC	40:40:22:89:1c:51
SID	0
LNID	9420
Level	0
State	Terminal
SSID	-
Coverage	99.20%
Connection Time	09-10 10:05
Disconnection Time	09-11 18:03
Availability	88.51%
Database	
<input type="button" value="Reload"/>	

Figura 140 – Información de un nodo de la subred


La interfaz web nos permite también programar tareas para grupos de contadores en intervalos periódicos de tiempo. Esta opción podrá ser configurada en la pestaña “Task scheduler”.


Programmed tasks (TP TAR) (1)


#	Task identifier (Task ID) ¹	Start time (TpHi) ²	Execution period (TpPer) ³	Priority (TpPrio) ⁴	TpCompl	
1	S02	2015/06/25,04:00:00S	1d	2	<input type="checkbox"/>	Delete
2	S04	2015/06/01,00:00:00S	1M	2	<input type="checkbox"/>	Delete
3	S05	2015/06/01,02:00:00S	00:02:00	2	<input type="checkbox"/>	Delete
4	Add					


Scheduled actions per task (TPPRO) (2)


#	Task identifier (Task ID) ⁵	Action (TpReq) ⁶	STG send (TpSend)	Storage R/W (TpStore)	TpAttr (Query ID)	TpAttr (Parameters)	
1	S02	S02 ▾	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			Delete
2	S04	S04 ▾	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			Delete
3	S05	S05 ▾	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			Delete
4	Add						


Advanced scheduled actions per task (TPPRO)

#	Task identifier (Task ID)	Action (TpReq)	STG send (TpSend)	Storage read/write (TpStore)
1	Add			


Scheduled gas actions per task (TPPRO)

#	Task identifier (Task ID)	Action (TpReq)	STG Send (TpSend)	Storage read/write (TpStore)
1	Add			


Meters per task (TPMET) (3)

#	Task identifier (Task ID) ⁷	Meters serial number (TpMet) ⁸	
1	S02	ZIV0042540112,ZIV0042540113,ZIV0042540114,ZIV00	Delete

Figura 141 – Planificador de tareas

En esta vista podemos fijar el intervalo de periodicidad de cada tarea programada (1), pero para ello antes debemos establecer un identificador para las tareas a realizar (2) y añadir los contadores sobre los que queremos realizar cada tarea (3).